HOUSE OF LORDS

SELECT COMMITTEE ON COMMUNICATIONS

Regulating in a digital world

Oral and written evidence

Contents

The Adam Smith Institute & Entrepreneurs Network – written evidence (IRN0070)

Written evidence to be found under the Entrepreneurs Network

Advertising Association – written evidence (IRN0039)

About the Advertising Association

1. The Advertising Association brings together the whole of the advertising and marketing communications industry, including the advertisers, the agencies and the media owners, along with nearly thirty trade association representing advertising, media and marketing.

2. Every £1 spent on advertising generates £6 to UK GDP and so advertising is a driver of economic growth, generating more than £120bn per year for GDP, and supports the wider creative industries. Nearly one million jobs in communities right across the country are supported by advertising services. The UK is a world-class hub for advertising, with the latest available figures also showing exports of British ad services reached a record high of £5.8bn in 2016.

3. We welcome the opportunity to respond to the House of Lords Communications Committee inquiry. Our response answers Question 1 of the inquiry, setting out the current regulatory framework, the challenges facing the advertising industry, the extensive self-regulatory initiatives that are already in place or in development, and recommendations for Government support.

Context

4. Digital advertising is a vibrant and successful sector delivering brand value and powering a significant proportion of the UK's digital and creative economy. Advertising is the primary tool to monetise content online and is therefore essential to a sustainable digital advertising industry, a free and open web and viable ad-funded business models (e.g. news).

5. UK digital advertising leads Europe. The £10.3bn spent on digital advertising in 2016 in the UK represents a market that larger than its German and French counterparts combined.

6. We share the Government's ambition to make the UK the best and safest place for online advertising. We want the country to represent a gold standard in digital for others to admire, follow and emulate and ensure that the UK retains its leading role in ecommerce and digital advertising.

7. In November 2017 the Advertising Association submitted a response to the Government's Digital Charter. The conclusions set out in this submission reflect the conclusions reached in that document that are most relevant to the Committee's inquiry.

Regulatory framework

8. Legislation regulating activity on the internet originates both domestically and internationally, vis-à-vis EU law and European judicial rulings. We

support the maintenance of the current regulatory framework, which includes the General Data Protection Regulation, the forthcoming e-Privacy Regulation, the e-Commerce Regulations and the Consumer Protection from Unfair Trading Regulations (CPRs).

9. All relevant UK legislation now accounts for activities within digital sphere. Internet intermediaries face liability under a range of UK legislation, for instance the Defamation Act.[1] Hence, while there is no internet law per se, there is a host of legislation at both UK and EU level applying to online platforms and intermediaries – the internet is not a 'wild west'. The right to be forgotten, for example, derives from a European Court of Justice ruling and affirms the right of individuals to request the removal of search engine results which are irrelevant or no longer relevant.[2]

10. The advertising and media ecosystem needs scale in order to be sustainable in the long term. Services need to continue to be provided seamlessly across multiple markets in the future. Future regulatory efforts focused on the internet should therefore maintain sight of the trans-frontier nature of the medium.

11. The free flow of data between the EU and the UK after the UK exits the EU is crucial to this long-term sustainability. The EU's General Data Protection Regulation (GDPR) will apply in all EU Member States from 25 May 2018 and the industry is preparing for implementation. Due to the sensitive nature of processing personal data, and the associated reputational cost and financial sanctions for errors, the advertising ecosystem is investing heavily in ensuring that data privacy is at the core of its activities. Cross-industry work is taking place to ensure that there is a consistent approach to GDPR implementation and that the UK will be able to demonstrate best practice standards of compliance.

12. The proposed e-Privacy Regulation threatens the future of the data-driven digital economy and could greatly undermine the investments made in GDPR implementation efforts. It is crucial that the UK continues to be closely involved with EU negotiations on the Regulation.

13. Following Brexit, UK businesses will in practice have to continue to adhere to the GDPR, and the forthcoming e-Privacy Regulation, to ensure continued provision of services to EU users. The Government should prioritise an UK-EU data sharing agreement, building on the existing 'adequacy model', as part of Brexit negotiations in order to ensure a continued free flow of data across borders. We welcome the clarification from the Government in the Prime Minister's Mansion House speech that the Government will seek "more than just an adequacy arrangement."

14. We welcome that the Lords Communications Committee report on its inquiry on UK advertising in a digital age (HL paper 116) supported our

[1] While this Act offers a defence to website operators who can demonstrate they were not responsible for the material posted online, the intermediary could potentially be liable if the poster is anonymous.

[2] *Google Spain v AEPD and Mario Costeja González*

position that the ICO should retain a place on the European Data Protection Board following the UK's exit from the EU.

Existing self-regulatory initiatives

15. Rapidly changing technology and consumer habits create new challenges for the advertising ecosystem. There are extensive self-regulatory initiatives already in place or in development to address these challenges, which are set out below. The final section of our response highlights ways in which Government could support these industry efforts.

16. The UK's self-regulatory advertising framework – administered by the Advertising Standards Authority (ASA) – already covers all digital advertising. The industry is committed to maintaining an effective self-regulatory system and is currently in discussions to ensure its sustainable funding. Self-regulation is a crucial element in making and keeping the UK a leader in digital advertising and serves as a blueprint for successful advertising regulation in many markets around the world.

17. Our industry is committed to playing its part in achieving the Government's goal of making the UK the best and safest place to be online, by focusing on addressing issues that can undermine consumer and business trust in digital advertising, including ad fraud and ad misplacement.[3]

18. There are a number of existing cross-industry initiatives which aim to address these issues. For example, the industry has developed a cross-industry self-regulatory initiative, the Display Trading Standards Group (DTSG) that is governed by the Joint Industry Committee for Web Standards in the UK and Ireland (JICWEBS)[4]. The DTSG has developed tools to provide transparency and enable buyers actively to manage campaigns and minimise the risk of ad misplacement.

19. The DTSG has published good practice principles for all business models involved in buying, selling and facilitating digital display advertising. There are currently over 60 signatories, covering a significant proportion of the market.

20. To minimise the risk of advertising funding IP-infringing content, the industry has worked with the City of London Police's Intellectual Property Crime Unit (PIPCU) to develop and implement the 'Infringing Website List' (IWL) that functions in effect as a 'blacklist' of sites that the Police have verified to be infringing copyright. This list enables the industry then to disrupt the ad revenue such sites receive. The DTSG provides a framework for the IWL to be used by the industry.

[3] **Ad fraud** is the deliberate generation of fraudulent (often non-human) traffic (i.e. visits to an online site/page, etc.) in an attempt to extract money from the advertising ecosystem. **Ad misplacement** is legitimate advertising being inadvertently placed next to content that is unsuitable for the brand (e.g. content that is inappropriate, harmful, or illegal).

[4] JICWEBS was created by the media industry in the UK and Ireland to ensure the independent development of standards to support best practice for online ad trading. More information can be found here: www.jicwebs.org

21. In March 2017, a new joint initiative was announced between JICWEBS and the U.S.-based Trustworthy Accountability Group (TAG)[5]. In the area of ad fraud, TAG has set up the Certified Against Fraud Program, involving anti-fraud guidelines, and a trust seal which means companies can publicly communicate their commitment to combatting fraudulent non-human traffic in the digital advertising supply chain.

22. JICWEBS and TAG are focused on transferring learnings between the respective initiatives to improve their effectiveness and create a united and consistent approach across markets to tackle criminal activity and clean up the digital ad supply chain.

23. Separately, the IAB Tech Lab – an independent research and development consortium that develops global technical standards for the digital advertising industry – last year published the ads.txt initiative. This project is part of a broader effort to reduce the ability to profit from intentionally misrepresenting inventory (known as 'domain spoofing') by providing a simple solution for publishers to declare who is authorised to sell their advertising inventory, and is being rolled out in the UK.

24. Tightening up procedures and guidance has been a number one issue for the industry bodies and companies in recent months, in order to minimise, if not wholly eliminate the problem. The industry is exploring how to build on the DTSG framework, including though the partnership between JICWEBS and TAG.

Conclusion

25. Ad-funded business models support the development and provision of digital services, content, and apps. The Advertising Association and its members are committed to supporting Government as it works to make the UK the safest place to be online, through continuing to develop effective self-regulatory solutions.

26. In our response to the Government's Digital Charter, we suggested a number of ways in which Government could support ongoing industry efforts:

Ad fraud

27. Engage with industry initiatives such as JICWEBS and TAG to support the continued development of industry solutions to address ad fraud in the digital ecosystem.

28. Work with industry better to assess the scale of ad fraud in the UK.

29. Allocate police response to build understanding and expertise in criminal ad fraud through the National Cyber Crime Unit.

[5] https://iabuk.net/about/press/archive/tag-and-jicwebs-partner-to-clean-up-digital-advertising-supply-chain

Ad misplacement

30. Develop an information sharing mechanism with industry to ensure that Government is aware of continuing industry efforts and discussions to minimise advertising misplacement, both domestically and globally.

31. Support the continued development and adoption of the best self-regulatory solutions to managing ad misplacement by all parties in the advertising ecosystem. For example, the Brand Safety Principles published by DTSG (the Display Trading Standards Group), which is the preferred mechanism of the advertisers represented by ISBA, the agencies represented by the IPA, the advertising technology companies represented by the IAB and the Association of Online Publishers.

32. Work at the international level to encourage other key markets to strengthen measures to address ad misplacement, notably on foreign language content sites which may be accessed by UK citizens.

Data: privacy and cross-border data flows

33. Encourage clarity from Data Protection Authorities, including the ICO, on forthcoming GDPR guidance on key issues. We welcome the guidance that has been issued by the WP29 and ICO since the publication of our Digital Charter document.

34. Prioritise UK-EU and UK-U.S. data sharing agreements as part of Brexit considerations. We welcome the clarification from the Prime Minister's Mansion House speech that the Government will seek "more than just an adequacy arrangement."

35. Work with industry to develop common thinking on future compliance issues as a result of opinions issued by the European Data Protection Board.

36. Continue investing sufficient resources into advocating for a pragmatic approach to the proposed ePrivacy Regulation.

37. Encourage ICO support for voluntary industry approaches, if any sector chooses to explore this, both in the UK[6] and at European and international level.

38. Ensure that the Data Protection Bill and other implementing legislation implements comprehensive GDPR exemptions for freedom of expression and information and other derogations including those vital to free flow of data across borders.

[6] For example, through support for effective implementation of membership codes of practice (e.g. DMA, MRS).

Ad blocking

39. Maintain equivalence with EU 'net neutrality' rules that require internet service providers to "treat all traffic equally" as it is directed over their networks. Net neutrality is an important principle that protects against network-level ad blocking (such as at mobile network operator level) and existing guidelines, based on the EU 'Universal Service Directive', state that all internet users should have equal access to content and advertising online to ensure telecoms operators cannot block content.[7]

40. Support publisher efforts to clarify legal avenues to challenge the lawfulness of disrupting legitimate business models through non-user led ad blocking mechanisms.

11 May 2018

[7] http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules

Airbnb – written evidence (IRN0091)

Airbnb welcomes the Committee's inquiry on the future of internet regulation. Developing strong and balanced legislative and regulatory frameworks for online services is a necessary condition for the UK to prosper economically and socially in a modern, globalised world. We are delighted to contribute to the inquiry and to offer our perspective on how this can be achieved.

Founded in 2008, Airbnb provides an online marketplace that offers access to around four million places to stay, and more than ten thousand local experiences, in more than 191 countries. Hosts choose to list their accommodation or experience on our platform and travellers book their trip through our website or app. Airbnb activity is spread across every nation and region of the UK. In the last year, UK hosts welcomed nearly six million guests and the Airbnb community contributed around £3.5 billion to the UK economy.

Our vision is to contribute to a world where anyone can belong anywhere: that a traveller to any corner of the globe can make a real connection with the place they are visiting, and to the people they meet there. Making this vision a reality will require us to focus on all of the stakeholders with whom we have a relationship: not just our employees and shareholders, and not just our community of guests and hosts – but also the communities where we create an impact.

Airbnb believes that the regulation of the internet in general, and of online platforms in particular, should promote innovation, investment and competition. This will ensure that citizens, businesses and government continue to be able to reap the benefits of the digital economy.

Online platforms benefit today's digital economy and society by increasing the choices available to consumers and creating and shaping new markets. Many online platforms act as facilitators between parties, providing consumers and businesses alike with access to a global market.

Any regulatory framework will need to be effective in protecting consumers and promoting fair competition. But it will also need to ensure an attractive regulatory environment for the development of online and digital business in the UK. In our view there are four key principles that should inform the future contours of internet regulation in the UK.

First, there should be a recognition that 'the internet' is incredibly broad and diverse. It cannot be regulated as a whole; there is no one-size-fits-all regulatory solution. Such an approach would seriously jeopardise the UK's prospects of capitalising on the opportunities created by the internet and wider technological developments.

The idea of introducing "specific regulation for the internet" is, therefore, something of a misnomer. There is huge diversity in internet companies and services, and online platforms and their activities. This should be reflected in the regulation that governs them, particularly in the fast-changing environment of the digital world.

This is particularly true for online platforms. A proper understanding of how platforms vary in functionality and business model is vital to the success of any regulatory framework. Imposing generic requirements on all online platforms risks restricting innovative business models. For instance, platforms that generate their revenue from the collection and processing of user data (e.g. selling targeted advertising) raise fundamentally different regulatory questions from e-commerce platforms who are connecting buyers and sellers of physical goods and real-world services.

While some cross-sectoral regulation may be appropriate (for instance, on data privacy) it is also true that some online platforms are already an integral part of their underlying industry and regulated by specific frameworks that apply to all participants in those economic sectors.

Second, new regulatory frameworks that take a suitably nuanced approach are beneficial for both businesses and consumers. A 'wild west' free-for-all is not in the interests of good online platforms or their users. Responsible platforms accept their role creates certain obligations to buyers, sellers and other stakeholders. Further, a clear regulatory framework allows firms to compete with one another on a level playing field.

As such, the debate should be less over whether there should be regulation at all but rather over what distinguishes good regulation from bad. Good regulation would distinguish between different 'sectors' of the internet. These include e-commerce, media, search engines, communications, payment systems, labour provision, operating systems, transport, advertising, distribution of cultural content and social networks. Each will require its own approach, reflecting that so many economic sectors now have both online and offline dimensions. It is almost always more meaningful to consider the "vertical" sector impacted by internet technology, rather than looking "horizontally" across platforms that may share very little in common.

Third, the UK ought to embrace rules after Brexit that are compatible with EU law to the greatest degree possible. Online platforms are inherently borderless. Some of the most popular internet services with British consumers are provided through platforms based in EU member states. Where services are very similar or identical across borders, regulation should be too. Regulatory divergence will likely create barriers to doing business in the UK, even if the motivating force behind such divergence is liberalisation.

Central to this is the EU e-Commerce Directive. As the inquiry's Call for Evidence noted, the Directive created the legal framework for online services in the European Single Market. Given the technological developments of recent years it is evident that the EU will need to clarify and update the e-Commerce Directive soon.

To allow online platforms to comply with their responsibilities, this reform will need to focus on a sectoral, problem-driven approach that maintains a balanced and predictable framework for online platforms and their users. Following Brexit, the UK will likely benefit from remaining closely aligned with the EU in the approach it takes to this important area of reform, particularly in the interest of consumers in the UK.

Fourth, the need to avoid regulatory fragmentation between the UK and the EU is mirrored by the need to avoid fragmentation within the UK itself. In the absence of clear and binding frameworks at national level, there is a risk of a patchwork of different regulatory requirements, which may inhibit innovation and competition.

We strongly support the Committee’s commitment to contribute to a greater understanding of how internet and online platforms can impact on the economy and broader society. We are an online platform that believes in taking responsibility for our community and our interactions with the world. We believe that users and platforms alike would benefit from forward-looking regulatory frameworks that recognise the differences between different types of online services and which encourage innovation, investment and competition.

18 May 2018

Professor Pinar Akman, Dr Orla Lynskey and Dr Nicolo Zingales – oral evidence (QQ 83-92)

Tuesday 26 June 2018

Watch the meeting

Members present: Lord Gilbert of Panteg (Chairman); Lord Allen of Kensington; Baroness Benjamin; Lord Bishop of Chelmsford; Baroness Chisholm of Owlpen; Viscount Colville of Culross; Lord Goodlad; Lord Gordon of Strathblane; Baroness Kidron; Baroness Quin.

Evidence Session No. 10 Heard in Public Questions 83 - 92

Examination of witnesses

Professor Pinar Akman, Professor of Competition Law, University of Leeds; Dr Orla Lynskey, Assistant Professor of Law, LSE Law; Dr Nicolo Zingales, Lecturer in Competition and Information Law, University of Sussex.

Q83 **The Chairman:** I welcome our witnesses to the House of Lords inquiry into regulation of the internet. Today's session is being broadcast online and a transcript will be taken. Our witnesses today are competition law experts. We are very grateful to you for taking the time to give evidence to the Committee. Could you briefly introduce yourselves and tell us a bit about your background?

Professor Pinar Akman: My Lord Chairman, thank you for the invitation. I am honoured to be here. I am a professor of law specialising in competition law at the University of Leeds, where I am also director of the Centre for Business Law and Practice. I work in areas of digital technology and the application of competition law to digital platforms. My background is in the prohibition of abuse of dominance in particular, and I have authored several articles and a monograph on the topic. I have been awarded the Philip Leverhulme prize in law, which I am going to use to look further into questions raised by digital platforms and the application of competition law.

In the interests of full disclosure, in case it comes up later, in the past I conducted one piece of research commissioned by Google. It concerned the then ongoing investigation of the European Commission into Google's practices, which culminated in an infringement decision.

Dr Orla Lynskey: Many thanks for inviting me here this afternoon. I am an assistant professor of law at the London School of Economics, and I work and research primarily in the area of data protection law. In particular, my main piece of research has focused on the limits of individual control over personal data. That has brought me to consider structural or holistic approaches to the effective protection of individual rights in the digital context. As a result, I have conducted research in recent years on the concept of digital dominance or data dominance, and looked at the interplay between data protection law and competition law, and in part consumer protection law, in the digital environment.

Dr Nicolo Zingales: I am very grateful for the invitation and am honoured to have the opportunity to give evidence on this important topic. I am a lecturer in competition law as well as in information law. I deal with online platforms from both perspectives, with regard both to the challenges they pose to traditional competition analysis and to their role and responsibility in ensuring the effective protection of user rights. In that regard, I am the co-founder and co-ordinator of the Dynamic Coalition on Platform Responsibility, which is a forum of individuals from different constituencies who discuss the role and responsibility of online platforms.

In the interests of disclosure, I am a co-founder of MyData, which is an initiative that ensures that individuals have more control over personal data, and can make more informed choices and derive knowledge.

Finally, on one occasion I too was funded by Google, but it was not for a specific paper; it was for a summer fellowship. I raise it in the interests of full disclosure.

Q84 **The Chairman:** Thank you to all our witnesses for introducing themselves.

The scale and dominance of the big platforms is the subject of a lot of media attention, public debate and policy-making. In the view of our witnesses, is the dominance of digital platforms a genuine issue for public concern? Perhaps we could have a brief perspective from each witness.

Professor Pinar Akman: As a competition lawyer, I do not think that dominance and market power on their own are a cause for concern. In the economic literature and numerous studies on this topic to date, what matters is the conduct adopted by companies that might earn market power. Pretty much all modern competition law around the world is based on that principle, so having market power, even at the level of dominance, is not on its own a cause for concern. What would be a cause for concern is if companies engage in conduct that is anti-competitive, distorts competition and ultimately harms consumers.

Size on its own does not tell us much. We do not know whether the size is the result of superior efficiency and being better than one’s rivals or the result of anti-competitive conduct. Modern competition law takes the view that size on its own does not tell us anything about the outcome as such. It might be a sign or a result of superiority or efficiency, and as long as it is not the result of an anti-competitive practice we would not be concerned.

Other factors to take into account would be barriers to entry to a market and whether, for example, consumers are multi-homing; whether there are switching costs; and whether there is access to capital. Can new entrants come into the market and challenge the incumbent? In the digital context, a recent study conducted by BEIS found that effective entry does not appear less likely in concentrated markets in the digital world. It looked at five case studies from the digital economy and found that sometimes concentration made entry more likely, because the bounty at the end in being successful in this market was larger than the bounty would be if there was more competition in the market.

We do not know whether there is an ultimate amount of concentration in innovation, but, on the basis of at least one study conducted recently, we know that concentration on its own does not make entry—which means new competition—less likely to occur. That is where I would stand as a competition lawyer.

Dr Orla Lynskey: Competition law is relevant in so far as it is the primary legal instrument available to us to regulate and constrain private market power in any way. However, competition law is not designed with the intention of remedying human rights problems or other problems that fall outside the remit of the concept of consumer welfare.

One potential source of unease is that firms occupying a position of strong market power might not simply be engaged in harmful economic conduct, which would be effectively constrained by competition law provisions. It might equally impact on the effectiveness of rights in other ways. It might not be a competition problem, but human rights problems might flow from the dominance of certain firms. I will give two examples.

A digital giant such as Google might have a direct impact on fundamental rights through the way it processes personal information in the context of its many services. However, it also has an indirect impact on the level of rights protections offered throughout the digital environment, because, for instance, it has a chokehold, or it is a gatekeeper for access to its own platform.

A mobile phone has an operating system, which in the case of Google is the Android operating system. In order for apps to be available on the Android operating system, Google will have an influence over the terms and conditions offered by those apps. In that way, dominant digital firms have the potential for a particularly powerful influence over the effectiveness of all forms of rights in the digital environment—autonomy, data protection, freedom of expression, et cetera—and that is where the unease comes from.

Dr Nicolo Zingales: I agree with what has just been said about the important role platforms play in impacting fundamental rights. Specifically with regard to that, there is a distinction to be made between different types of platforms. When we talk about a notional platform, I would argue that some of these entities are a more critical architecture for the freedom of expression and interaction of users—for example, app stores and search engines come to mind as particularly important in that regard. The problem with the existence of a concentrated market is not so much the scale and dominant position of companies but the framework that we have for detecting possible infringement of the law. We do not have a co-ordinated structure to deal with the range of issues that gives rise to.

I do not want to pre-empt my answer to other questions in that direction, but, as part of a team, in 2014 I conducted research into the terms of service of online platforms, which is one way to measure the exercise of market power by platforms. We found very problematic terms that kept users from an effective right to be heard in cases when content was removed. The terms deprived users of the right to access the courts and imposed a waiver on class actions, as well as mandatory jurisdiction in California on most occasions.

In general, the information that platforms provided about personal data they collected was quite insufficient. That is one example where there is no equal bargaining power between the two parties. As you know, users accept terms of service without reading them, and, even if they read them, they might not have the ability to understand them.

A further problem is that we cannot just rely on terms of service, as the platforms are constantly nudging us in one direction or another, and they effectively implement law through code. We need a system that is able to detect violations that occur through code, and allows users the opportunity to participate in the process and understand whether something that has happened to them is fair and legitimate, or is an abuse.

Lord Gordon of Strathblane: Is there something about the internet that has a built-in tendency to dominance—a virtual monopoly? You go from 51% market share to over 90% market share overnight.

Professor Pinar Akman: Indeed, and that is the result of network effects. On the internet, once somebody comes up with a product that becomes popular, there is almost a snowball effect; users attract more users. In an advertising-funded platform, users attract advertisers, so in a way success is exponential.

The study I mentioned earlier found that it also works in the other direction. If a platform starts losing users, it seems to lead to a rapid decline in some platforms that are no longer as popular as they used to be—for example, Yahoo in the search area, and Friendster in social networking. Success comes very quickly. An author has said that it has never been so easy to make a billion, but it has also never been so difficult to make a million. When you are successful, you are incredibly successful, but finding a product or a service seems to be the crucial thing.

Dr Orla Lynskey: Data has a role to play as well. There is a very lively debate at the moment among competition scholars and others about whether or not the possession of data on individuals, in particular the volume and variety of data, would lead to an advantage that could ultimately become a barrier to entry for potential competitors. That could be relevant in a single market. For instance, Google could use data in the context of Google Search to consolidate its position there, but it could also use that data in neighbouring or emerging markets. Competition authorities are struggling with how to treat that data.

Lord Gordon of Strathblane: What I am hearing suggests that, provided the barriers to entry are not impaired, you are not particularly worried about Google having, say, 94% market share in the UK.

Professor Pinar Akman: I would respectfully disagree with the point about data. Google itself had no data when it started, whereas Yahoo, the incumbent at the time, had loads of data. The same goes for the social networks that existed before Facebook. Google and Facebook were themselves new entrants in markets where there was an incumbent with data. It seems that data may not be the key factor that enables or prevents entry. In today's world, there are institutions in the business of data. You can buy data. There are diminishing returns of scale with data. You need only so much data to work out what consumers prefer. In my opinion, as long as the entry barriers are not insurmountable, I would expect competition to do its work.

Dr Nicolo Zingales: The example of Google and Yahoo is particularly interesting. Yahoo was well ahead in the quality of its results. The big mistake it made was to sell its traffic to Google. By saying, "We are going to power our searches through Google", it basically lost its competitive edge. This market is driven by scale, which is at the basis of the search industry. Now it has taken a further step, which is data, because searches are personalised. It is not only scale, which may indeed legitimate the presence of one or few players in the market because you need a lot of traffic to get accurate results; today, personalisation increasingly plays a role.

Lord Gordon of Strathblane: If a large dominant company buys a new entrant, is that automatically construed as anti-competitive, or just as a Christmas bonus for the new entrant?

Professor Pinar Akman: That is an important question. At the moment, we may not have the right competition tools to deal with it. We have examples where incumbents have bought new entrants—innovative companies that have something really different. Some of them have escaped scrutiny in competition law, because merger rules, as we have them at the moment, do not always have the capability to scrutinise such deals. It happens particularly when the two companies do not appear at face value to be competitors, but it might be an area that the incumbent may consider going into. That is important and it is something competition authorities will need to deal with.

It is possible that the rules may need to change so that such deals can be scrutinised so that they do not kill competition. We should remember that some new entrants may be innovating simply because they want to be acquired by Google. We need to think about the possibility that, if the deals are prevented, those innovations may not happen. I do not know whether we have enough evidence to work out which way it is at the moment, but it is definitely something we should be looking into.

Baroness Quin: I want to pick up a point Dr Lynskey made. Do you think the platforms recognise that they have an effect on human rights, or is it something they largely ignore?

To piggyback on my colleague's question, how easy is it to scrutinise the kind of deal you mentioned? How easy is it to scrutinise something that on the face of it seems very opaque—at least to me?

Dr Nicolo Zingales: On the first point, which was directed to Dr Lynskey, I increasingly participate in conferences where representatives of platforms talk about what they are doing to give effective protection to fundamental rights, so they recognise that. Even at UN level, the special rapporteur on freedom of expression issued a report this year that said it was increasingly concerned about the lack of transparency.

Platforms have recently come up with a declaration about how they are moderating content. They are taking steps, but so far they are baby steps. There is increasing political pressure and recognition on their part, but it would be good if they had specific procedures in place to show that they have accountability by design.

On the second point, there is a very difficult question. To go back to one of the arguments that was made, data has a key role. It can easily move from one market to another; it can be used to build new services. Therefore, when there is an acquisition by a player that might not be in the same market but has many users and much information about what they are doing, that information can be used in another market. There needs to be more attention paid to those kinds of acquisitions. A good example is Facebook’s acquisition of WhatsApp.

More generally, a problem with the accumulation of data by platforms is that they have much more information about how the markets are going to evolve. Quite often, they see their competitors before those competitors or anyone else, even the competition authorities, realise they are a threat, and they buy them. I am not sure what the solution to that would be, other than to say that perhaps we should rely more on the knowledge that the platforms have. Rather than referring to general understanding in the industry, we should have a more subjective analysis of what they are doing. That answers only part of your question.

The Chairman: Dr Lynskey, do you want to deal with the issue of human rights?

Dr Orla Lynskey: If I may, I will go a bit further and deal with just one right: data protection or privacy. I recognise that we should not speak of platforms as a single entity because there is a lot of internal differentiation in their business models, how they are monetised and so on, and that merits consideration. However, in the sphere of data protection a platform would simply say, “This is a regulated area and, therefore, our scope for manoeuvre is quite limited”. That pushes the question back: if an area is not functioning effectively for individuals, it is because there is a market failure.

The rules introduced under the new general data protection regulation apply across the board, potentially to me as an individual processing personal data, in the same way as to Google. There are some differences as regards accountability, the need for documentation and so on, but in general the legislative framework that we have at present, in that sphere in particular, does not put special responsibility on firms that, because of their ubiquity or reach, might be particularly impactful on rights.

There is at least a case to consider a type of special responsibility for rights protection analogous to the special responsibility on dominant firms that we see in competition law, because everything they do has such a significant impact downstream, or on the market. You could make that analogy and say that that type of special responsibility should be extended across the board to the rights area, because the logic that everything they do has a more significant impact extends across the board to societal effects, including economic ones but going beyond them.

Professor Pinar Akman: On Baroness Quin's question about how to scrutinise a merger when an incumbent buys an innovative firm, you are absolutely right that it is particularly difficult in dynamic markets to predict what is going to happen in the future and how competition will evolve. That was submitted by the Competition and Markets Authority in its evidence to this Committee. In a way, merger control is always about gazing into a crystal ball, because it is always prospective. Whenever a competition authority looks at a merger, it tries to predict what will happen in the future in that market.

One thing that authorities around the world are considering for this type of merger is transaction value. Currently, merger rules do not catch that aspect of the transaction; we look at the turnover of the parties, and in the UK we can also look at the share of supply of the parties, but we do not look at the transaction value.

A good question is why an incumbent is paying billions to purchase a new company that was established just last month. That suggests to us that the company thinks there is something to look at, and that is one thing for competition authorities to consider.

Viscount Colville of Culross: I do not know whether it is possible to do this briefly, but I will direct this question to you, Dr Zingales, because you do work that looks at the user-platform interface.

We are looking at the dominance of ownership of platforms. Is it possible for Governments to nudge the market so that more user or publicly or co-operatively-owned platforms, where there is empowerment of workers, users and citizens, determine what happens on the internet? Is there anything that Governments can do and anything that we can suggest?

Dr Nicolo Zingales: In that respect, the Government have already tried to do something with regard to the so-called Midata initiative. They suggested that consumers should have access to their personal data. Going back to the initiative that I co-founded, MyData, the principle is that all data should not go exclusively to the platforms. An alternative solution is that platforms have access to data generated through them, but that data must be given to consumers as well, which would enable them to create decentralised structures that can move to other platforms to connect.

That alternative model is increasingly being advocated as part of data co-operatives. A number of individuals establish the rules and try to protect certain fundamental values—for example, workers' rights and personal data protection. It is a model that I would definitely recommend taking into consideration because it does not require the same level of intervention that is advocated against the dominance of platforms: it suggests that perhaps we can harness the power of the market and empower consumers to switch very easily, which is connected to your inquiry's interest in data portability, and make more informed choices, as well as knowing the terms and conditions that will apply throughout their activity on the platform. At the moment, vague and sometimes quite unfair terms are being used against them, and we do not know how they are being implemented. If we switch to this model, users would be able to establish their own terms and conditions and then allow third-party platforms to connect to their ecosystems only if they fulfil those terms and conditions, so you flip the model around.

Viscount Colville of Culross: That is interesting.

The Chairman: That is a very interesting area. We may want to explore it a bit later, or on some other occasion.

Q85 **Baroness Kidron:** The other side of the equation is how the regulators see it. Would you say briefly what you think the position of the regulators is? We keep getting evidence about price, but perhaps they are not using some of the other qualities that are at their disposal. We would be very interested to hear from you on that.

More importantly perhaps, do you think the current system is suitable for the digital environment? We are thinking particularly about end-to-end services that do not necessarily look dominant but might dominate a user's experience as well as a market.

There is also the question of jurisdiction. Professor Akman, you have already brought up the question of mergers. Could each of you look at the regulators' current position and what tools may be missing from their toolbox?

Professor Pinar Akman: If I may, I will start with the Competition and Markets Authority as the competition regulator. The competition rules are flexible—perhaps too flexible—and could be applied to any set of circumstances. They are very short principles and rather vague. We may be lacking some of the tools with which to apply those rules to the digital markets that we have.

One particular example, which is quite fundamental, has to do with the point you made about price. Usual competition analysis is built on the idea of price and market power being defined as the ability profitably to increase price. That causes a serious problem for some of the online platforms that we are looking at today, because they are actually offering their services for free to the users. This is a serious problem for competition law assessment.

Any competition assessment, particularly on dominance, starts with defining the relevant markets: what is the product market that we are looking at? We cannot define dominance in the abstract; we have to establish what the product or service is. Because these markets are two-sided, and remuneration is coming only from one side, which in the case of, say, search engines is advertisers, there is difficulty in figuring out whether we look at the users' side, at the users and the advertisers, or at the advertisers' side because they are the ones paying for the service. For example, in the United States, court decisions have held that there cannot be an anti-trust market when the product is free, and that is the end of the inquiry. Obviously, courts and authorities in Europe have taken a different view, but it is a serious essential question to be dealt with at the beginning.

Unfortunately, I do not think that currently we have the tools to answer such questions with the required precision. That is one example where the competition authority, as the regulator, will be challenged when looking at the digital market. It will be similar with the role of data. Is big data a barrier to entry, or is it like any other input to a business? Because these firms are digital, their input is digital, in the form of data.

On efficiencies and the role of innovation, how much value does one put on innovation, which will obviously happen again in the future? There is competitive tension in the market, which is the usual way we think of competition; there are certain companies in the market and they compete in that market. There is also competition for the market, which is a far more dynamic perspective of competition, and that has to take innovation into account. How much emphasis to put on the role of innovation in competition law assessments is a challenge to the competition authorities at the moment.

Dr Orla Lynskey: Another challenge, in the context of a free market, is that, if we take the emphasis away from price, we are left to consider other parameters of competition: innovation, quality and choice. A lot of work has been done recently on how to measure improvements or disimprovements of quality. A digital product such as WhatsApp's communication application is priced at zero, so how can we tell, after its acquisition by Facebook, whether it has improved or disimproved in quality? You might say that the quality of the data protection policy has lessened as a result of the transaction. However, it might have improved aspects such as data security, because it now benefits from Facebook's data security infrastructure. Internally, when considering quality, there will be a lot of incommensurables or things that are very difficult to measure one against the other.

In some instances, competition analysis in digital markets might have blind spots simply because a lot of the focus is on the impact of a particular conduct or transaction on actual or potential competitors, whereas, for mergers, as has already been highlighted by the Committee, a lot of the acquisitions are taking place in parallel markets, and that falls into the blind spots of competition analysis.

If I think about that from my data protection perspective, I see the acquisition by big platforms of firms that are not direct or potential competitors, but are data processors in peripheral markets that are being gathered up slowly but surely. No one transaction is causing a big stir, but, when you look at the overall picture afterwards, you see large-scale data aggregation from a wide variety of sources.

In my research, I have argued that we should be considering whether or not to use tools that are parallel or complementary to competition tools, such as the public interest test in the context of mergers, to assess that type of transaction. That type of test is currently used primarily in the context of media mergers, but we might be able to make some sort of analogy with the data protection context and say that the economic outcome of the transaction is not the sole consideration. We might also consider the broader societal impact of the transaction, and whether there might be implications down the line for individual autonomy, freedom of expression, data protection or choice, simply in the digital environment. That might merit further consideration.

The Chairman: Do you have anything to add, Dr Zingales?

Dr Nicolo Zingales: I agree with everything that has been said, but I have two further points. I agree that it is difficult to measure the impact on innovation and quality; it is much more difficult than with prices. If we think about predatory pricing, there is a clear rule; if you price your product on a measure below your costs, you basically aim to exclude your competitor from the market. It is difficult to pursue that kind of specific reasoning with regard to quality, and for example with regard to data protection, which is increasingly a measure of quality.

In that respect, the GDPR will bring more clarity—for example, through codes of conduct[8] that could set out different levels of protection for personal data in different circumstances. That could be a way to measure quality.

Another purely competition issue is that often the benefit brought by certain restrictions of competition in one market flows into another market. If we think about the free market that users get, there might be some restriction on the advertising side that enables the provision of the service for free. Or there’s the classic case of credit card companies, which impose a certain restriction on their merchants in order to offer their service uniformly. That is a big question for competition law, and there was a decision in the Supreme Court yesterday on that very issue. It is not exactly clear how we evaluate cross-market efficiencies. Currently, EU competition law tends to be quite focused on one market and does not allow one to take efficiencies in another market into account as long as the consumers in the two markets are substantially different. They need substantial commonality of consumers to take into account the benefit in the other market.

Baroness Kidron: I note that in Australia competition law sits with the consumer and competition regulator; they are one and the same. That may provide a more holistic approach to some of these issues. Are you nodding in agreement or recognition?

Professor Pinar Akman: Yes, both recognition and agreement with the principle that it might be far more useful to have broad powers within the same authority.

The Chairman: Are the other witnesses nodding in agreement?

Dr Orla Lynskey: Yes.

[8] In conjunction with certification mechanisms and a robust framework for detecting and punishing deviations from the prescribed conduct.

Dr Nicolo Zingales: Yes.

Q86 **Baroness Chisholm of Owlpen:** We have already heard a bit about conduct, dominance, transaction values and empowering consumers to move. I would like to take that a bit further. What do you feel about competition law assessments? Do they strike the right balance between short-term efficiencies and innovation?

Professor Pinar Akman: This is a very difficult question, because it requires us to know quite a bit about the counterfactual world on which we almost always have no information. Ex post assessment of competition interventions is very rare. In cases where there has been an infringement decision and a company has, let us say, stopped whatever the infringing conduct was, and in cases where there has been a non-infringement decision, we never know what the actual impact has been on long-term innovation, so it is very difficult to answer.

At the moment, the authorities I am familiar with, such as the European Commission, are more concentrated on short-term efficiencies, and the longer in the future the alleged efficiencies are, the less weight they are likely to be given in traditional competition law assessment. One example is the Microsoft case, which found an infringement against Microsoft in the EU some years ago. Microsoft took great pains to argue that, if the EU proceeded in the way it was proceeding, there would be a detrimental effect on Microsoft's incentives to innovate. Its rivals might innovate, but what about its incentive to innovate as the current dominant company? That was not well received.

Where innovation is taken into account, it is usually in favour of the competitors of the incumbent, as opposed to looking at the innovation that might come from the incumbent itself. Several commentators noted that, looking at the Microsoft investigations in the US and in the EU, if those interventions into Microsoft's conduct had not taken place, Microsoft today might have been a far more serious competitor to Google, for example. It is very difficult to know.

Dr Nicolo Zingales: I broadly agree. We need to recognise, as was also mentioned in the previous question, the concept of system competition. You need to take into account that the incentive set up by having a company take part in multiple lines of businesses may be undermined if you focus on a very narrow market.

I also believe that the concept of nudging is powerful. The regulator should not be too strict on a company favouring one product or service over another, which was complained about in the Google case. There is some merit in scrutinising those kinds of practices—preferential placement—but, on the other hand, attention needs to be paid to the fact that algorithms constantly nudge us in all sorts of directions and that it is the role of the algorithm to detect what goes first and what goes second. You cannot adopt too mechanistic an approach to scrutinising that kind of practice. I do not know whether that is clear to the panel. I think it is one of the major challenges. I am arguing that it would undermine innovation to apply it too mechanistically without a de minimis exception, for example. Perhaps I can comment on the framework that needs to be set out to address that kind of practice in later questions.

Q87 **Viscount Colville of Culross:** You have explained some of the problems in dealing with competition law in the digital markets. I would very much like you to address what can be done. What reforms could be made to existing competition legislation to enhance the competitive process?

Professor Akman and Dr Lynskey, you talked about the difficulties of competition authorities looking at the ecosystems in too narrow a way, and often there is a parallel purchase and a parallel market that did not understand the effect. You explained earlier that a smaller company might be acquired outside the existing ecosystem and could have an unexpected effect.

Dr Zingales, you said that companies had more data than the regulators could have, so they understood better where the market was going. How could we nudge and change the legislation to help the regulators?

Dr Orla Lynskey: Competition law is the only legal tool we have, aside from economic regulation, to deal with dominance. In some ways, we are putting a lot of emphasis on competition law to expand and face a lot of problems within its remit. Competition law will deal with these issues case by case, so there is always the risk, which Professor Akman alluded to, that if you intervene at one level, for instance in the way I advocated in the merger context by having a public interest assessment of data-driven mergers, you might have unintended consequences from that type of intervention.

For instance, if you intervened in the data-driven context, you would say that aggregation by a dominant firm such as Facebook of entities such as Instagram and WhatsApp will lead to an aggregated dataset that is too large, reveals too much and gives too many insights about individuals. At the same time, competitors might say, as was argued in the US in the AT&T merger, "We need to merge in order to have exactly that kind of dataset at our disposal. We need that competitive insight in order to compete". By disallowing that transaction in the UK or the EU, you might have a situation where it is allowed in the US. There would be competing claims that in my opinion would be impossible for any one competition authority to deal with, and to foresee the broader consequences for the market.

What does that point to as a response? There could be more collaboration between competition authorities, with an overall structural assessment of how the internet will function as a market now and in the future. That is obviously a huge exercise, but you can see from a lot of the economic literature that we are plagued by uncertainty.

The big question is whether we believe there will be another Schumpeter wave of destruction that sees existing firms wiped out of the market, or whether we will have entrenched dominance for the foreseeable future. We need more research on that question.

More immediately, we could see more collaboration between different regulators already operating in the digital sphere, so that there is no duplication of effort and everyone is on the same page about where their competencies overlap. In the UK, that could be the Information Commissioner, Ofcom, the CMA and various others. There are many instances where competencies overlap, and they are increasing. I can give some examples if that is helpful.

Viscount Colville of Culross: Are you suggesting that there should be a super-regulator that covers all those things? Would that solve the problem?

Dr Orla Lynskey: I do not know whether you would need an entirely new regulatory body. Dr Zingales has been involved in the idea of a digital clearing house, which has been proposed at EU level. In that instance, it was foreseen that there would be co-operation between competition, consumer protection and data protection policies, in a very loose co-operation mechanism, just to see where their areas of interest overlap.

Professor Akman has already mentioned that competition authorities might consider the question of a dominant firm extracting a lot of data from individuals. That might be problematic from a competition perspective, but it could also be a data protection question, or a consumer protection question. The very same legal problems would be analysed through different lenses. There is scope to join up thinking on how to deal with that type of issue, which is central to how we as individuals experience the internet.

The Chairman: Can I ask the witnesses to be reasonably brief? We are quite pressed for time. You have given us lots of evidence and there is more to come.

Professor Pinar Akman: Some of the issues we have mentioned with the application of the rules in digital markets will be resolved only through enforcement and case law. While that is happening, economics can catch up by offering us economic analysis of what is or can be happening in some of those markets, because economics underlies pretty much all competition law and enforcement. The problem is that economics and the law are lagging behind actual technological developments. The problem with enforcement is that it takes years, and by the time we have a decision the market has completely changed.

We should also bear in mind that it is possible that there is no competition law problem. It could be that competition is working effectively. Several authorities around the world are looking hard to find problems in these markets. If there are problems, I am certain that they will find them. The fact that we have not had much enforcement might be an indication that there is no competition law problem.

As to what authorities can do to innovate to stay more in line with the innovative companies they are looking at, they could set up their own data units, as the CMA is doing. They could use algorithms to catch conduct that is taking place through the use of algorithms in the markets, which the EU Commission has alluded to. There are ways in which the authorities can innovate to stay in tune with the markets.

Dr Nicolo Zingales: To add briefly to Dr Lynskey's point, the digital clearing house is an important example of collaboration, but the authorities need to co-operate not only at the level of exchanging possible ideas, theories about market definition and so on; they should collaborate on specific cases. Quite often, a data protection issue comes up in a competition law investigation, and the authority is not sure how to deal with it. It might not have the power to pass that information to other authorities, so that might be where we need a specific co-operation agreement between different authorities. The authority might not have the ability to assess the issue, even within competition analysis, and give it the appropriate qualification from a data protection perspective, so that calls for a more integrated approach to specific cases.

Q88 **Lord Goodlad:** I have two questions. First, in your view, what principles or criteria should determine users' right to data portability and platform account deletion? Secondly, could greater data portability and interoperability mitigate the control that the dominant platforms currently exercise over personal data?

The Chairman: Can we start with Dr Lynskey? You have addressed some of these issues partially, but please add to them.

Dr Orla Lynskey: Data portability is underpinned in principle by the idea of individual control over personal data. The new Data Protection Act in the UK, which reflects the general data protection regulation, seeks to give individuals more effective control over their personal data, which is where initiatives such as MyData come into play, because they allow individuals to do something with that data.

Will that be effective, or lead to interoperability? Data portability is one thing, but it does not necessarily mean interoperability. Interoperability means that, if I have my data on one platform and you have yours on another, we can interact with it; for instance, I could be on Facebook and Dr Zingales could be on a different social networking service, and we could communicate. Although that might unlock markets, it could be problematic from a data protection perspective, because it leads to data duplication. There are questions about whose privacy policy and whose terms of use prevail in those circumstances. That might be an example where you need joined-up thinking about what would be the best way to proceed and whether or not you force interoperability.

Dr Nicolo Zingales: I agree. Data portability and control is not a panacea, much like transparency, because users often do not have the ability to appreciate all the circumstances, and they might not exercise their control adequately. The problem with data portability is that quite often data relates to other individuals, so we might want to make sure that users use such data appropriately.

As regards affecting dominance and improving the situation in the market, one needs to bear in mind that there is always the possibility that, if the labour that has been put into a platform is taken to another platform, it might undermine the incentive to produce that labour in the first place, which is why the general data protection regulation does not apply to so-called inferred data; it applies only to data provided by the user or observed on the platform by users of the platform. It would probably be far-fetched to require the platform to give all the structures it has for the user to be able to port them anywhere else.

With regard to the difference between portability and interoperability, interoperability is a different concept that requires much more effort; it requires collaboration, because the application programme interfaces are constantly updated. A basic standard needs to be set, probably across the industry, and updated with technological development. It is much more difficult to achieve that. Portability goes some way to improve the situation, but it does not resolve the problems of lock-in and switching costs in moving to another platform.

Q89 **Lord Goodlad:** How do you think GDPR will impact, if at all, on competition law or competitive assessments?

Professor Pinar Akman: My colleagues will be able to add more on the details of the regulation, but, if I may, I will make a small point. GDPR may have an adverse effect on competition in the market, because it is a very extensive and detailed regulation, which obviously will come at great cost to small businesses, and potentially new entrants, in the market where it applies.

Regulation itself can create entry barriers for new entrants, and GDPR may be an example; you may have come across websites that literally stopped operating in the EU when GDPR entered into force, because they were not in compliance. For companies such as Google and Facebook it is going to be far easier to comply with GDPR, but for new and small companies, which could challenge those large companies, compliance will come at a greater cost.

Dr Orla Lynskey: I may differ slightly on that point. GDPR may increase the costs of doing business in so far as any regulation, such as labour law regulation, increases the cost of doing business. GDPR scales the obligations it imposes depending on the scale of the data processing operation. If you have a company with five people but you are doing large-scale data analytics, the accountability obligations and other features that are imposed on you will be significant, but rightly so, I believe.

As to how it might influence the competitive environment, it is something that competition authorities need to be aware of when assessing competition in the market. We may see the possibility of companies starting to compete effectively with one another on the basis of the data protection conditions they offer users, because to date we have not seen that type of competition emerging. For instance, now we are seeing models where businesses are saying, "You can have less analysis of your data by making a micropayment for this service, or full-scale data analytics and the service for free". There could be other issues with that, because in essence we are pushing the responsibility back on individuals to pay for their data protection, so minimum standards would still need to be in place.

Dr Nicolo Zingales: I do not have much to add, other than a point on the complaints that GDPR is affecting competition in the market because small companies cannot cope with all the regulations. The regulation is indeed imposing some obligations across the board, which are essential for it to be effective, and then it imposes an asymmetric type of regulation where there is a lot more emphasis on the capabilities and impact of data controllers. They will need to exercise a greater level of care, which I think favours the small players, who will simply have to comply with minimum requirements.

Q90 **Baroness Quin:** Given that most competition regulation is currently carried out at EU level, will there be problems for the UK post Brexit in relation to enforcement of competition law, or, given what you have said about the importance of co-operation between authorities, is it likely that we will be very closely aligned to the EU in any case?

Secondly, in the new post-Brexit world, will a UK regulator be able to take effective enforcement action against US-based companies?

Professor Pinar Akman: That is another great question. I had the honour of giving evidence to the EU Sub-Committee on the Internal Market on the issue of Brexit and competition. Two things came out of that process.

First, resources are very important. Unless the CMA’s resources are increased proportionately to the expected increase in its workload, it simply will not be able to cope with the workload. There will be a whole set of mergers that the CMA will need to look at, which currently it does not because of the one-stop-shop system whereby the EU Commission deals with cross-border mergers.

Another really important point that came out of that process was that co-operation will be essential. The CMA will need co-operation agreements with key stakeholders such as the EU, the US and other jurisdictions, because several of the issues will be cross-border. How will the CMA go into another jurisdiction to collect evidence of an infringement? If it takes a decision, how will it enforce that decision in a foreign jurisdiction?

Those things can be resolved only through co-operation agreements between the CMA and the other stakeholders. When the UK leaves the EU, presumably the CMA will no longer be a member of the European competition network, which is currently the network that enables such information sharing and co-operation with member state competition authorities. I only hope that there will be some alternative arrangement that will put the CMA on that footing after the UK leaves the EU.

In principle, the rules can be effectively enforced against US-based companies. In practice, it will depend a lot on the resources that the CMA has and its ability to enforce its decisions in foreign jurisdictions and collect evidence in foreign jurisdictions.

The Chairman: We have a couple of questions left. The Lord Bishop will ask questions and then Lord Allen will ask a further question. I will ask you to respond to Lord Allen’s question in writing, but I would like to put it on record.

Q91 **Lord Bishop of Chelmsford:** You have already touched on some of these issues, but you may wish to add something. Do you think competition law could alleviate the need for other forms of internet regulation? I am very mindful of your brief but affirmative answer to Baroness Kidron earlier, which may be relevant here. Could the consumer welfare standard be amended to encompass the non-economic concerns that you also mentioned earlier? Obviously, this is not just about price.

Dr Nicolo Zingales: There is increasing understanding that consumer welfare might encompass some non-economic objective, but what is often missed in the debate is the nuance of when the consumer welfare standard becomes relevant. The two key moments during competition analysis when it can be a factor are at the stage of justification of conduct and in the imposition of remedies. Why do I say that?

Often, a company might be pursuing one of the fundamental rights objectives or might be mandated by law to undertake a certain action. That action might be justified on the basis of something that is not strictly economic. For example, if companies agree that they might set standards of access to their platforms, on the basis of privacy, to preserve that kind of value, it might be a legitimate justification, or what is called an objective justification in competition law.

The other element where it is particularly relevant to look at other areas is that, when the competition authority imposes a remedy, it has the duty to make sure that it is not infringing other rights. When it imposes the remedy, it should bear in mind that it has to craft the remedy in such a way that it preserves, for example, the data protection and intellectual property not only of the company in question but also of third parties.

The problem with the discussion is that often it simply refers to the fact that the standard by which we should judge conduct is not an economic one, and we should pursue all sorts of values as the ultimate objective of competition law. The objective of competition law is primarily economic. At EU competition law level, we also have market integration objectives, and the query is what we will do after Brexit in that regard. However, I would caution against putting it all together in one basket, specifically because it would create an unpredictable standard and some policy leverage that is also very inappropriate for the allocation of competencies, the rule of law and legal certainty.

Professor Pinar Akman: In my opinion, the consumer welfare standard should not be amended to encompass any non-economic concerns. That is not because the consumer welfare standard is perfect; it is far from perfect, but, of the other options we have, it is the most concrete, if that is the right expression. If we include other concerns that might be more political or might have to do with issues that the competition authority cannot really deal with in its assessment, we turn the business environment into a very uncertain one, which will put off businesses from investment and innovation.

According to the Enterprise and Regulatory Reform Act, which established the Competition and Markets Authority, "The CMA must seek to promote competition, both within and outside the United Kingdom, for the benefit of consumers". That is the guiding principle in the legislation. I think it is the right one, and we should stick to it in future.

The Chairman: Dr Lynskey, you have the last word.

Dr Orla Lynskey: I simply concur with what has just been said.

The Chairman: That is very precise. Thank you very much. You have given us a lot of evidence. One of the things you talked about earlier was the need for co-ordination of regulations. I am going to ask Lord Allen to put a question on the record. Given that time is pressing, I will then ask you to respond to it briefly in writing.

Q92 **Lord Allen of Kensington:** As we know, there is a plethora of regulators on the internet. I would like your views on two things. First, do you think there is a need for an ombudsman for consumer complaints? Would that be helpful?

Secondly, there seems to be quite a gap where we are playing catch-up all the time as new platforms and models are coming out. We had examples about blockchain changing the world. Is there a need for a regulator with a role in working with the industry in horizon planning? If you think there is, would that be best served through a new regulatory body, giving existing regulators more authority, and, as we have just heard, a co-ordinating role to bring things together, so there is not the level of conflict we currently see with regulation across the internet?

The Chairman: If you would be so kind as to respond to us on that in writing, we would be very grateful. If there is anything else that you think we might have asked but did not, or anything you might have said if I had not been pressing you so hard to speed up on occasions, we would welcome it. The evidence has been very useful and informative for the Committee. Thank you very much for giving us your time today.

All Rise Say No to Cyber Abuse – written evidence (IRN0037)

Introduction

1. All Rise Say No to Cyber Abuse (ALL RISE), welcomes the Select Committee inquiry into how regulation of the internet can be improved, with the backdrop of the government's Digital Charter, committing to make the UK the safest place to be online, whilst increasing trust in technology.

2. ALL RISE notes the focus on building a foundation upon which the UK digital economy can thrive. ALL RISE puts forward that an *economy* can only thrive when the *people* thrive, and that is at the core of this submission.

3. There has been a recognised call to action to address the out of control human calculated hate, abuse, harassment and pure manipulation that takes place through the tool of the internet. The measures currently in place to protect people from this abuse and bring perpetrators to justice are wholly inadequate and failing to meet the most basic duty of care.

4. Through the work of this inquiry, the government has an opportunity to instigate true change: to bring responsibility and respect back to our human interactions and to raise the bar in our standard of decency on and offline. That is the standard we will carry with us into the future, for the generations to come. The UK can lead the way in this.

5. We offer our support to the Select Committee on this subject and would be happy to participate in oral representations in relation to the Call for Evidence or otherwise. In the meantime, please let us know if there are questions or clarifications we can address or further information we can provide.

Background

6. ALL RISE is a not for profit organisation with the purpose to address the epidemic crisis of cyber abuse globally, including via research, education and better regulation wherever needed.

7. Cyber abuse is taking a devastating toll on all facets of life. For victims, for those around them and for wider society in the UK and beyond. And it is far from being solely a youth issue.

8. In a 2015 All Rise global survey of more than 12,000 participants, 72% of contributors had witnessed cyber abuse and 1 in 3 had witnessed it at least 6 times. 38% had suffered cyber abuse themselves. We have all seen the onslaught of press coverage, cases and statistics on cyber abuse since then.

9. 40% of the world's population – more than 3.5 billion people - use the internet. Even on a conservative extrapolation, the size of the problem is clear and its magnitude cannot be underestimated. Rates of anxiety, depression and suicide are continuously on the rise and at levels never previously recorded. It cannot be ignored that social media is increasingly cited as having a huge impact on our human health and wellbeing.

10. Cyber abuse is in fact an emerging international public health concern.

11. Research into the true harm is nascent, but shows, for example, that countries with higher rates of cyber abuse are more likely to have high incidences of child death – with a 1% rise in the prevalence of cyber abuse translating to a 28% increased risk of unnatural child death. In addition to physical and psychological harm, cyber abuse is being linked to emotional distress, depression, suicide, anxiety and conduct issues, such as use of alcohol and cigarettes, plus retaliatory violence[9], not to mention the serious physical and mental health[10] risk factor that ultimately has an impact on each of us in the offline world.

12. Our health and wellbeing are worth more than constantly accommodating a reduced quality of life in how we treat one another.

13. A societal reset on a major scale is needed to bring us back to a standard of communication and interaction we all deserve, and that can be precipitated by decisive legislative change and direction, policing and prosecution prioritization on cyber abuse, as well as a dramatic shift in responsibility on the part of the online platforms that provide our modern-day community spaces – spaces that should be safe for all.

[9] Patchin & Hinduja, 2006; Raskauskas & Stoltz, 2007; Shariff & Hoff, 2007; Sourander et al., 2010; Wang, Nansel, & Iannotti, 2011; Ybarra & Mitchell, 2004

[10] As Paula Todd writes in her book Extreme Mean, 'My research revealed that the problem with cyberabuse is far, far bigger, that it is affecting adults, everybody. Not just being the target of cyberabuse but reading it and being exposed to it all the time is bad for us. We already have a mental health problem around the world... we are building a social and mental health crisis.'

Call for Evidence Questions

1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

Building clear responsibility into the law

14. There are currently 12+ pieces of legislation implicated in cyber abuse. It could be said these laws make adequate provision to address online abuse. However, it is not working – cyber abuse is spreading like an infectious disease, unabated. The perception is that online abuse is something to be tolerated, not addressed head on. Police and prosecutors are working with uncertainty and complexity in the law. Victims are unable to get access to justice, save in the most extreme cases or if they have the wherewithal to bring an expensive civil claim privately.

15. Decisive action is needed, to bring forward specific legislation to put the illegality of cyber abuse and the consequences for committing it beyond doubt, as well as to increase the sanctions in order to communicate with clarity the policy position of this country to say no to cyber abuse. ALL RISE proposes the following:

    - Make it clear the criminal standard for online and offline behaviour are the same. Update the Public Order Act 1986 to put it beyond doubt that cyber abuse is a public order offence.
    - Increase the sentence to 5+ years' prison and a significant fine, with publicity around the shift, to make crystal clear the seriousness of cyber abuse and provide a deterrent effect.
    - Provide for the equivalent of 'on the spot' fines, as per offline public order offences and issue guidance to law enforcement to be fulsome in their use.
    - Consolidate the 12 pieces of legislation that are currently implicated in cyber abuse into a single, fit for purpose law.

16. The current trajectory is towards self regulation by the online platforms. Due to internal bias, self-interest and cross border issues, this will not bring the necessary accountability or bring the UK government the necessary jurisdiction for it to discharge its duty of care to its citizens, nor to those suffering abuse at the hands of UK nationals.

17. The internet has emerged from its 'start up', early innovation phase – 50%+ of the world's population is now online and the positive and negative impacts of the internet have become clear. Regulation is now able to address the clear issues that have arisen, and it can be applied appropriately and proportionately. This path to regulation is a well-worn in other industries. For example, broadcast media and the development of clear and appropriate regulation to ensure consistent standards are set, understood and adhered to for the content we see on TV and radio. Or in the context of pollution and waste management, where strong and strengthening regulation has been introduced for corporations over time, as the harm of different industries emerged. Online abuse is itself a

pollutant and one for which the clean-up is currently being carried by health services, law enforcement, communities, families and businesses, but not by the online platforms where the abuse is generated and taking place.

18. Regulation has been shown to be effective and often necessary to bring about change. Recent examples are the plastic bag levy and the update to the Criminal Justice and Courts Act to address 'revenge porn'. These developments were based on a glaring need for change and clear data on the harm being caused. What is clear with cyber abuse is that the current state of play cannot continue, where only the most extreme cases are prosecuted or only people with influence or wealth can access justice via civil cases or have the benefit of a higher standard of moderation by the platforms. New criminal regulation would provide a clear and level playing field for all.

19. Strong regulation is needed, to stabilise the important tool of the internet and re-establish the foundation for all of us in our use of that tool in how we interact, share ideas, debate and disseminate information. These are critical pillars in our democracy. If we do not act, those pillars become degraded, along with the richness of discourse and decency that is available to all of us.

Anonymity

20. In addition, the issue of anonymity online needs to be addressed.

21. There is marked difference in the accepted standards of behaviour between our online and offline reality. Online, we see, experience, endure and accept abuse we simply would not deliver or tolerate face to face. This is the result of:

    - A Toxic 'Online Disinhibition' effect – meaning there is a dissociation caused by anonymity. That there is a restriction of how much you truly know of a person and this means when there is engagement with a computer or a faceless name onscreen, we feel removed from the fact that we are interacting with a real human being who has real feelings.

    - A sense of actual or perceived invisibility in front of the law, denoting that you can 'hide behind the screen' and not be held accountable for your actions.

22. A high proportion of cyber abuse would never take place if perpetrators knew they could be easily identified and in fact that their identifying information would be disclosed to their victim or the authorities acting on their behalf, in the event of abuse. It is therefore fundamental to look at what is causing the sense of anonymity and separation. The reasons include:

- The lack of basic 'know your customer' (KYC) checks on users - currently online platforms do not know with any certainty who their customers actually are.
- The use of pseudonyms as usernames.
- The fact that users can have multiple accounts, all with different names.
- How difficult, if not impossible, it is for victims to establish the identity of those who abuse them, which means they cannot arrest the harm being done to them or have basic access to justice.

23. ALL RISE proposes the introduction of a driver's licence for the internet. This would cut these problems at the core and immediately increase the level of responsibility we have online, as well as eradiating anonymity, or rather the sense of anonymity. Each of us gets a licence to post online and if we break the law, we lose that licence. An internet licence would also facilitate proper KYC checks by the online platforms, which would become the expected norm.

24. Addressing anonymity is fundamental and must be embraced as part of the Select Committee's review.

Independent body

25. Currently, online platforms decide what is and is not acceptable as regards the content and behaviour we all see and experience online. It is their terms and conditions and 'community standards' or rather their discretion as to those standards, that prevail. Those terms purport to put personal safety and protection at the core, yet in practice, the bias is towards freedom of speech at all costs - freedom from harm is rarely if ever considered.

26. In practice, we have no baseline regarding content and behaviour that is and is not acceptable and legal online. We have the promise of this baseline in the words of the 'community standards' communicated to us all via the online platforms. However, in practice, these standards mean nothing – they are inconsistently and inadequately applied and policed. This is clear to see from a simple search of content on any one of the platforms, and this is also evidenced in a research project undertaken by ALL RISE. A summary of this research is set out at Annex 2 and more information can be provided on request.

27. What is needed is to take the decision-making as to our baseline standards of human interaction and legality out of the hands of a select group of invested, commercial organisations and into the hands of the government or a cohort of governments globally, representing us all. What is needed is an independent body to set the standard and ensure it is maintained, as well as to adjudicate on complex cases, undertake regular audits, preside over appeals and to provide transparency as to the state of play and progress. Other countries, for example New Zealand and Australia, have established independent agencies or Commissioners to begin to bring accountability and oversight back into

the hands of the government and local judiciary and away from commercial organisations with conflicts of interest.

28. ALL RISE offers itself to establish, administer or otherwise support that independent body.

Freedom of speech

29. Clarification is also needed as regards freedom of speech. Frequently, free speech is put forward as the reasoning behind tolerated levels of abuse online. Freedom of speech is critical to modern society and must be respected and protected. Yet freedom of speech is by no means freedom to abuse, nor does it mean freedom to harm – an inalienable right to say what you want with no constraint or accountability. If as a society we are limited in our ability to have respectful discussions or disagreements with people without resorting to abuse or harm, this clearly indicates the pure reductionist value placed on each individual's own right to be free to choose the life they want.

30. Human rights run both ways and freedom of speech cannot be prioritized over personal safety and privacy (Article 2 and 12 of the Universal Declaration on Human Rights, not to mention the overarching importance of brotherhood (Article 1).

31. There has arisen an important opportunity to clarify what freedom of speech actually means as regards our communication online, and the responsibilities that come with that and, critically, the limitations on all of us as we engage in a free and respectful society. Freedom of speech must not be used to justify cyber abuse.

32. Further context on freedom of speech can be found in Annex 1.

2. What should the legal liability of online platforms be for the content that they host?

33. The Ecommerce Directive was introduced in what now feels like a bygone era. The focus was on protecting and ensuring innovation and a competitive market. In many ways the legislation achieved its goals, although from a competition perspective, few EU companies punch with the same weight as the US incumbents.

34. One of the biggest winners from the Ecommerce Directive has been the online platforms. They can provide services to millions of people worldwide, harvest their data and make millions in revenue, and yet have zero responsibility for what their customers see and experience and the harm they suffer whilst under their care. Yes, the platforms have to remove illegal content once they are notified, but they have no obligation proactively to stop that content from reaching our eyes and ears, even if they know their sites are full of it. And in the name of free speech, they have discretion to play off laws against one another, in order to remove the least material possible, which results in the provision of the least level of protection for consumers.

35. The claim is that we must suffer indecency, disrespect, personal attacks, harassment and other forms of abuse, in order to protect free speech. ALL RISE asserts this to be an entirely flawed position. In fact, the massive cyber abuse happening across the world every day is itself killing free speech and itself bringing about the 'chilling effect' so often feared when we consider free speech. Voices are crushed and people stop speaking their truth, many too hurt and afraid even to be online.

36. With the initial 'start up' phase of the internet long since passed, the question now has to be asked: **what is needed from the law for the next phase of the internet?**

37. ALL RISE puts forward that it is time to shift the position on liability for online platforms. The 'figuring it out' or 'sandbox' phase is over. Liability must sit with those who host the content and have the wherewithal to know in detail every piece of content and data on every user on their network. The position is very different from an ISP who is simply allowing content to pass along its pipes as a 'mere conduit'. For hosted content, the responsibility must be to provide a service that is free of harm, in the same way we expect of those who provide our shopping centers – hence the health and safety standards and the security guards. By removing the liability 'safe harbour' for hosting, those in charge of these online environments will have a clear obligation to police them and they can discharge that responsibility by deploying best practice standards, tools, technology and processes.

38. There is a huge amount of data and personal experience shared day in, day out regarding the volume and severity of abuse online and the harm it causes. To see this volume is to know this is a subject on which urgent action is needed. The trajectory points to a catastrophic effect – to fail to act now would be to see the iceberg in the distance and fail to turn the ship.

3. How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

39. As referenced above and set out in Annex 2, research undertaken by ALL RISE shows that content moderation by online platforms is consistently inadequate and often grossly negligent. There is no transparency, accountability, consistency or clarity in the decisions that are taken and certainly no access to justice for those suffering harm every day as a result. The platforms will often serve those who are well known or well connected with a higher level of service in regards to abusive content and behavior, with content removed more quickly or abusive accounts suspended, which, whilst being disappointing from a fairness and access to justice point of view, also shows what can be achieved if the motivation is there.

40. To correct this, see above the proposal for an independent body to set the standard, oversee compliance and handle appeals regarding content moderation.

41. As regards transparency and appeals, there are well established processes online that can be drawn on, for example in copyright infringement cases. Where content is removed as abusive, a notice can be applied in place of that content, to make it clear the content has been removed and the reasons for the removal. The platform can also notify the person who posted the content, to educate them as to how the content or behaviour relating to the content was abusive and unacceptable. This will also give them an opportunity to appeal, for example if something has been posted fraudulently, in their name.

42. Consideration should also be given to limiting the number of accounts for a single user. The fact that users can have multiple accounts, all with different names, facilitates a variety of abusive behaviours. It is well known that trolls will attack a victim using different IDs to give the appearance of multiple attackers and increase fear and the volume and magnitude of abuse. They rely on being able to stay head of the moderators, who may close some abusive accounts but not others. When abusive accounts are closed down, trolls can simply open new ones with a new name.

43. The simple action to take is for the platforms to limit the number of accounts people can open against a single ID. Once that account limit has been met, people wanting further accounts can make a formal request with a valid reason, which be properly considered on a case by case basis.

4. What role should users play in establishing and maintaining online community standards for content and behaviour?

44. The state of the internet is the responsibility of all of us. As internet users, we play our part through the standard of our everyday

interactions and the content we post and with which we interact. We also have a responsibility as bystanders to abuse.

45. Do we see it, stand by and do nothing? Do we gloss over it, ignore it, become numb to it or stop even noticing it is there? Do we think 'nothing will happen if I report it so there is no point'. Like litter in the street or the person bad mouthing the bus driver, do we say 'this is just how things are'?

46. Or can we be reminded that we all make a difference – that every person matters and that every person can contribute to turning this around?

47. There are a number of laws around the world that impose a legal obligation on bystanders to act. An extreme example is complicity - if you knew a murder was planned and did nothing, you are complicit in that crime. Other examples are around the duty to rescue someone in peril, which is a common legal concept in Latin America. ALL RISE is not proposing to criminalise bystanders who are not participating in abuse. However, there is an opportunity to reset our behaviour around taking action to address abuse we all see online, at the very least by recording and reporting that abuse as bystanders and perhaps also via guidelines on how to step in with counter speech or support. A national campaign would be an effective way to bring about such a shift, as would a reporting helpline or tool via which bystanders can take meaningful action.

5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

Proactive content and behaviour moderation

48. Online platforms are already employing filtering, automated moderation tools and machine learning to address hate speech, extremist material and child abuse images. This investment is much needed and must be extended to other forms of online abuse such as harassment, bullying, fraud and personal attacks.

A Troll Register

49. Another critical aspect in addressing cyber abuse is the introduction of a troll register. For those who choose to attack or harm others with words or harassing behaviour online, there will be a very real consequence – their actions will be publicly recorded and known.

50. A framework for the troll register is set out in Annex 3.

6. What information should online platforms provide to users about the use of their personal data?

51. An important subject for consideration in relation to personal data, is access for victims to data about those who are subjecting them to harassment and other forms of abuse.

52. Current practice involves such data only being disclosed in response to a Norwich Pharmacal Order or via Mutual Legal Assistance Treaty or equivalent processes. These processes are lengthy, cumbersome and hard to come by, for all but the most wealthy, informed and/or well connected or only for those suffering such extreme and persistent abuse that the police are able to justify resourcing an investigation. This means most victims cannot identify their abusers and thus the abuse and the harm it causes can continue, unfettered.

53. A new and efficient process is needed, whereby victims of cyber abuse can know who is attacking them and use that data as evidence to bring the perpetrators to justice. The fact that the data is held in another jurisdiction can no longer be a bar to this basic access to justice.

54. If a UK national can use a service in another jurisdiction, whether for a fee, in exchange for the use of their data or in return for the sale of advertising against their profile, then the service provider has a duty of care to that person, even if they are resident in another jurisdiction and even if consumer protection or criminal laws are found lacking. There can be no more hiding behind a veil of cross border conflicts and bureaucracy.

55. The solution needed here is likely to be legislative, to impose a requirement on the social media platforms to disclose forthwith, in the event of a legitimate request for data, and not reliant on a police investigation or formal order of the court. If the victim can evidence abuse, the data identifying their abuser should be disclosed to them, or to a regulatory body with oversight in these cases, with or without police involvement. Acknowledgement is likely to be needed via an exemption in data protection legislation, to make it clear that reasonable evidence of abuse will be sufficient grounds for waiver of the perpetrator's right to privacy.

56. Given the current volume of cyber abuse cases, there is likely to be an initial spike in investigations flowing from proper access to perpetrator data and that would need adequate resource. The troll register may well reduce the need for such volume of cases.

7. In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

57. The online platforms have been 'working on' cyber abuse for many years, with no meaningful progress in sight. Full disclosure should be made to regulators and consumers globally as to:

- The amount of cyber abuse on the platform, i.e. what is the likelihood of suffering abuse and what proportion of abuse can a consumer expect to experience if they use the service.

- The measures in place actually to prevent cyber abuse from happening.
- Service levels committed to by the platforms in how and how quickly they moderate content and behaviour in cases of abuse.
- Full disclosure on the content that is reported as abusive but not removed and the reasons why.

58. This transparency can be overseen and facilitated by the independent body, proposed above.

8. What is the impact of the dominance of a small number of online platforms in certain online markets?

59. The dominance of the online platforms and the scale of their userbase, reduces the likelihood of consumers voting with their feet if they hear of, see or experience cyber abuse. With little competition, comes little motivation and little innovation in solving this problem. Cyber abuse is an issue to which smoke screens can continually be applied, giving the appearance of action, with no actual change happening.

9. What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

60. The General Data Protection Regulation has shown the power of the EU working as one, to effect change on a critical topic. The UK will need to be vigilant to keep step with such progress and ensure it does not languish behind in bringing forward what is needed.

61. However, the UK also has the potential to lead the way, notwithstanding Brexit. Take the approach of Germany, introducing the NetzDG law to ensure the prompt removal of hate speech and bilaterally impose fines for breach, including to online platforms in other jurisdictions, notably the US. Germany acted according to its own conscience and duty of care and this opportunity will remain for the UK after it leaves the EU.

Conclusion

62. The constant tolerance and acceptance of abusive language and pure hate thrown around as weapons, with deliberate intent to harm or destroy one another, is reaching epidemic proportions, with an unknown number of casualties. The Select Committee’s review into regulation of the internet is much needed in this context.

63. There are a number of initiatives that can lead the way in how we move forward to ensure the internet can be a foundational tool for all of us, now and for the future, rather than an environment in which illegality, degradation and abuse are allowed to fester, with the knock-on effects that has on our collective and individual wellbeing, communication and access to information.

64. ALL RISE proposes:

- New and consolidated legislation to bring together our online and offline standards – the standards we will and will not accept in this country, as regards the content and conduct we see and experience and the clear consequences for failure to meet those standards.

- The removal of the liability 'safe harbour' for online platforms for the content they host, to ensure responsibility sits where the harm is taking place.

- An independent body to provide accountability and oversight for compliance with that legislation.

- Clarity around the responsibilities that come with free speech and the balance between our right to speak freely and our right to live free from harm and fear.
- A troll register to bring a meaningful consequence to all who seek to abuse.

- Increased access for victims to data identifying those who perpetrate abuse against them.

ALL RISE looks forward to seeing progress on the Select Committee's work in this, and is available to participate in further discussion and provide any additional information or research data, as needed.

> *'What is a cyber-bully', cyber-abuser and or cyber stalker? He or she is a character who has abandoned any form of decency and respect and has instead adopted guerrilla style warfare - 21st Century style, keyboard weaponry. This is a person who has knowingly sought to hurt and defame with reckless intemperance. 'Freedom of Speech' and or 'qualified privilege' for this assailant is a far cry from the reality as clearly evidenced by their calculated intent, a catalogue that will exhibit no less than a pure focus to hurt and defame another or others at all costs.' – SB*

May 2018

ANNEX 1

FREEDOM OF SPEECH

Article 10 of the European Convention on Human Rights expressly states as follows:

> *The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*

The International Covenant on Civil and Political Rights and the American Convention on Human Rights also refer to the 'special duties and responsibilities' that come with the right to free expression, and refer to the imposition of liability as needed to ensure:

> *a.* *respect for the rights or reputations of others; or*
>
> *b.* *the protection of national security, public order, or public health or morals.*

As France describes it in the Declaration of the Rights of Man and of the Citizen:

> *Liberty consists in the freedom to do everything which injures no one else; hence the exercise of the natural rights of each man has no limits except those which assure to the other members of the society the enjoyment of the same rights.*
>
> *The free communication of ideas and opinions is one of the most precious of the rights of man. Every citizen may, accordingly, speak, write, and print with freedom, but shall be responsible for such abuses of this freedom as shall be defined by law.*

Legal systems around the world recognise the limits on freedom of speech in the context of the conflicts that can arise with other rights and values and there is a body of law to account for this. Hate speech, pornography, libel, slander, obscenity, incitement, confidentiality/trade secrets, public security, perjury, copyright infringement, privacy and holocaust denial are just some examples.

Not only does freedom of speech have its limits and responsibilities, but it also stands equal to other rights, for example freedom from fear. The right to live free of fear is enshrined in the Universal Declaration of Human Rights – it is described as one of the 'highest aspirations of the common people'. Franklin D Roosevelt cited it as one of the 'Four Freedoms'.

The International Convention on Civil and Political Rights specifically embodies:

The right to be free from cruel, inhuman and degrading treatment or punishment - article 7

The right to the highest attainable standard of physical and mental health - article 12

The right to work and have a fair and safe workplace (relevant to workplace cyber abuse) – articles 6/7

The right to privacy and protection against attacks upon honour or reputation – article 17

The right to security of the person – article 9.

ANNEX 2

ONLINE ‘COMMUNITY STANDARDS’ ARE NOT POLICED

ALL RISE has undertaken research into the enforcement of terms and conditions and community standards. As part of this research, hundreds of comments were reported on a daily basis for a month period. Ensuring that the researcher wasn’t seeking out abuse, the research was limited to normal hashtags, eg: women, men, the names of world cities etc. In September 2017, 260 tweets were reported which ranged from:

1. “Yeah, because of u parasites.”
2. “Stay where you fucking are and spend your shit pound. We certainly don’t want you or your kind anywhere near the eurozone. Cunt.”
3. “They will rape and enslave this child.”

Out of the 260 reported, only 32 tweets were removed. In January 2018, the same research was applied to 450 tweets. Examples of the reported tweets were:

1. Fuck you. Pay me. Anyone in toronto CRAVING to be abused.
2. This shitbag cums his pants when GOP members get hurt. What a fucking asshole.
3. Swedish teen upskirt (video).

Out of the 450 tweets only 2 were removed.

The lived truth is that, despite the current efforts of the platforms, cyber abuse goes unaddressed and furthermore is fertilized and growing within these environments. The notice and take down process is failing. Yes, it could be said that there are some cases where success is seen, but there are countless cases where victim after victim is being told the standard line “the comment does not breach our community standard”, even though the reported content contains threats of religious vilification, harassment and abuse.

There are countless examples and we will have all seen them in the press. In 2017 it was reported that MP’s within the UK received 190,000 tweets of abuse over a three-month period. Another example showed Rachel Riley walking away from her job as a Sky Sports Re- porter due to the abuse she received online Unfortunately, in these situations the common brush off line society uses in the absence of a higher standard, is that it is normal to be not liked if you choose to work in the limelight.

In addition, it has been well reported that non-celebrity victims and bystanders report abuse, yet nothing transpires. They will with optimism report abuse again, persistently, only to receive the response the “community standards are not in breach”.

Example 1:

In July 2017 a woman opened up her online account and found her face photoshopped into the crosshairs of a gunsight. The image was a screengrab of her profile page, taken by a user she had blocked. It showed her face directly in the center of a target above a caption that read, "@[username redacted] BTFO kill #390 #noscope" (BTFO is shorthand for "blown the fuck out"). Four days after filing the first report, she received a formal email from the platform. It said - @[username redacted] had not violated the platform's rules.

Example 2:

A man received 3000 posts from one single account. The agenda of the account holder evidently was to stalk, harass, vilify and condemn religious beliefs or behaviours, incite others to harm or stalk, acting relentlessly in this conduct.

When reported to the platform the response was:

> *Hello, Thank you for reporting this issue to us. Our goal is to create a safe environment for everyone on [the platform] to express themselves freely. We reviewed your report carefully and found that there was no violation of [the platform's] Rules regarding abusive behavior.*

In both examples a follow up response was sent – a plea of decency and respect being instigated or installed upon the platform to take responsibility for having put the perfect weapon of mass destruction and abuse into the hands of a criminal being held with no accountability - to all intents and purposes, invincible. Also an appeal to be free from harm, which is a constitutional right. Yet no change occurred - the harm was not addressed. Therefore, the question needs to be posed: have 'community standards' become nothing more than a tick box exercise whilst wiping hands clean of responsibility?

Consequently, this has meant hate speech, discrimination, pornography, child abuse material, misogyny, harassment, personal attacks and much more are justified and warranted to remain on the platform, after platforms have been personally appealed to and asked to remove it. Regardless of the challenges of the volume of content and abuse, people are seeking help and in many cases there is little to no response. On occasion where surface level action is implemented, abuse is muted only for the victim or reporter, but remains on the site for the rest of society to see, view and make comment.

Extensive examples of cyber abuse can be provided on request.

ANNEX 3

Troll Register – A Framework

Introduction

All Rise Say No To Cyber Abuse proposes the introduction of a public register of those who consistently choose to abuse online: a 'troll register'.

Cyber abuse is taking a devastating toll on all facets of life. For victims, for those around them and for wider society, on a global scale.

It is time to #RaiseTheStandard of our interactions online and the bar of what we deserve and accept in how we treat one another. A troll register is part of that standard re-set for all of us.

For those who choose to attack or harm others with words or harassing behaviour online, there will be a very real consequence – their actions will be publicly recorded and known.

The Purpose

The purpose of the troll register is to:

- Begin to bring significantly needed accountability online. If you choose to harm other members of society through word, using a platform as a tool to commit your abuse, then that behaviour will be publicly known. There will be an immediate consequence, as there is offline for that harming and abusive behaviour. Abuse remains a choice, but not one for which trolls escape consequence. This also has the potential to offer a significant deterrent effect for would-be trolls, who will think twice before acting in a way that could affect their employability and social standing.

- The register will support with transparency for victims. It is too often the case for victims that little to nothing is done about their harm online, unless the media scoop a story and the case gets escalated due to its profile. The register will validate the experience of victims and provide an indication that their reports have been recognised, recorded and are being actioned.

- It will also enable solidarity with other victims, who may feel a greater responsibility and motivation to stand up and act to say no and stop abuse, if they can see their abuser is already on the list as a known troll; there is a knowing they stand with others in their experience.

- The register will bring transparency in respect of the volume of trolls on the various networks and therefore the size of the challenge society is facing. Data regarding the register can be tracked for analytics, for example trends relating to geography and growth, spikes around world events and issues and the impact of cyber abuse measures implemented and enforcement activity.

The Troll Register – how it works

The exact implementation of the troll register will depend on the extent of involvement of the platform companies.

Full participation of the platform companies

When certain defined criteria are met, the relevant platform company will ensure users of abusive accounts have their account frozen and their names added to a public register maintained by the relevant platform, along with the category/ies of abuse they have perpetrated and the time period. This is self-initiated by the platform in response to abuse reported by victims and/or in response to a report from a local authority.

Each platform will maintain their register in accordance with an agreed specification, to ensure consistency of decision-making, transparency and data with other platforms, globally.

Technological solutions such as blockchain, can be considered, to ensure the cohesion and integrity of these registers.

No participation of the platform companies

When victims suffer cyber abuse, they will report that abuse to their relevant local authority. Where certain defined criteria are met, users of abusive accounts will have their names added to a public register maintained either by the relevant authority, along with the category/ies of abuse they have perpetrated and the time period.

The registrar will notify the relevant platform of the abuse, the user name, the time period and the fact that their customer has been included on the troll register. They will also request appropriate action be taken, such as deactivation of an account or cooperation with a police investigation.

Management of the troll register

The troll register shall be managed with the utmost integrity and transparency and subject to regular, independent audits.

Criteria for inclusion on the troll register

The following **behaviour/conduct** shall warrant inclusion on the troll register

- Harassment
- Stalking
- Inciting others to participate in discrimination and hatred
- Inciting others to make a personal attack
- Encouraging suicide

The following **content** shall warrant inclusion on the troll register:

- Threats
- Discrimination and hatred
- Obscenity

- Disclosure or misuse of personal data without consent, including private information and photographs
- False information, including malicious assertions and/or unsubstantiated accusations of criminality
- A personal attack

Removal from the Troll Register

An application can be made in the following circumstances, for removal of a name from the troll register.

1. Appeal process

   A rigorous appeals process is a critical facet of the register.
   If a person believes they have been wrongly included on the register and they are in fact innocent of cyber abuse, they can follow an appeal process requesting their name be removed.

   The following are the bases for appeal:

   - Identity theft and impersonation, whereby another person has perpetrated the abuse under your name
   - Mistaken identity, whereby you have been wrongly associated with the user profile/ID that has perpetrated abuse
   - Wrong categorisation, whereby you believe your actions did not amount to cyber abuse

   The appeal process will be overseen by a dedicated team, applying strict review criteria.

   The appeal process itself will be subject to regular, independent audit.

   If the appeal process results in a finding that a name was wrongly included on the troll register, a label will be applied against the name on the register to that effect. The name will be removed from the register after an agreed period thereafter.

   If the appeal process results in a finding that the name was correctly included on the troll register, a 'failed appeal' label will be applied against the name on the register.

2. Reparation

   If a person wishes to make amends for cyber abuse they have committed, they can follow a reparation process. The process will include:

   - acknowledgement of the behaviour that led to inclusion on the troll register
   - an unreserved apology to the victim
   - full cooperation with local law enforcement

- an ongoing commitment and regular re-certification process regarding a high standard of respectful behaviour and content standards online
- other such measures as may be appropriate on a case by case basis

Reparation processes will be subject to careful oversight and record keeping.

Those participating in a reparation process will have a label applied against their name on the register to that affect. The name will be removed from the register after an agreed period following the end of a successful reparation process.

3. Expiry

If after a period of 5 years from inclusion on the troll register, no further cyber abuse has been reported against the person behind the applicable name, the relevant name will be removed from the active register.

A person can apply for early removal if:

- after a period of 2 years from inclusion on the troll register, no further cyber abuse has been reported against the person behind the applicable name
- they commit to an ongoing, high standard of respectful behaviour and content standards online.

Alliance for Intellectual Property – written evidence (IRN0096)

Introduction

1. The Alliance for Intellectual Property welcomes the opportunity to respond to the Committee's consultation entitled 'The Internet: to regulate or not to regulate?'.

2. Members of the Alliance may make individual submissions and this is therefore intended as a high level response that seeks to answer some of the legislative policy questions in the consultations that impact on many Alliance members.

3. Established in 1998, the Alliance for Intellectual Property is a UK-based coalition of 20 organisations with an interest in ensuring intellectual property rights receive the protection they need and deserve. Our members include representatives of the audio visual, toy, music, games, business software, sports, brands, publishing, retailing and design industries.

4. The Alliance's overriding objective is to ensure that intellectual property ('IP') rights are valued in the UK and that a robust, efficient legislative and regulatory regime exists, which enables these rights to be properly protected.

5. Members work at a national and local level with law enforcement bodies to reduce the harm caused by intellectual property crime in local communities and ensure legitimate businesses and traders are able to operate fairly.

6. We also work closely with the UK Intellectual Property Office (IPO) to raise awareness of the harm caused by IP theft. We are participants in the IP Crime Group, which facilitates cross departmental dialogue and joint working amongst the relevant enforcement bodies and organisations and support the Police Intellectual Property Crime Unit (PIPCU) which is the world's first dedicated IP crime unit.

7. The Alliance is also proactive in supporting the promotion of IP through educational and consumer awareness initiatives and encouraging the development of IP training for businesses and individuals seeking to develop and produce goods, services and content. Alliance members have created various initiatives to support this strategy.

8. The licensing and registration of IP rights is the framework that allows for creativity to happen and enables rights holders to protect their IP and choose where and how to distribute and sell.

9. The UK also has one of the best developed and applied intellectual property regimes in the world. Creators and businesses have been able to use that framework to develop exciting and innovative products, designs and content using the latest technology and manufacturing techniques. The Taylor

Wessing Global Intellectual Property Index (GIPI5) ranks the UK third globally, while the 2017 US Chamber of Commerce International IP Index ranks the UK in second place.

10. The Internet has unquestionably changed the way we live our lives, interact with each other, buy and sell goods and services and how we work and enjoy our leisure time. The Internet affords immense opportunities for creators of IP in all forms to create, market, distribute and sell their goods, services and digital content to mass audiences globally and Alliance members' sectors have been at the forefront of technological change, developing new products, services and formats.

IP protection

11. The Alliance supports the need for IP rights holders to protect those rights wherever they are delivered or sold and many Alliance members are actively engaged in helping their sectors protect IP online through monitoring and enforcement activities.

12. The Alliance is a member of the IP Crime Group, which brings together Government and the private sector to share best practice and knowledge on how to enforce IP rights that are exploited for criminal gain by individuals and organised crime gangs. The Intellectual Property Office (IPO), Police, Trading Standards, HMRC, CPS, NCA, Border Force and other agencies all attend the Group and there has been a strong emphasis recently on dealing with online criminality.

13. In the UK, the Alliance has helped deliver and progress the Voluntary Code of Practice on Search [11] and also supports initiatives by law enforcement and industry to tackle piracy and counterfeiting, including Operation Jasper, Operation Creative and Operation Ashiko, the former run through the National Markets Group and the others are run by PIPCU.

14. In addition the recently published Creative Industries Sector Deal provides an opportunity to create new partnerships and agreements with a range of operators in the online space to tackle IP crime and infringements. In this document (published in March this year) the government has committed to further safeguard copyright content by bringing together online intermediaries and rights holders to consider the need for and agree new Codes of Practice on social media and user upload platforms, digital advertising and online market places (considering legislative backstops if sufficient voluntary progress is not made by the end of 2018). The Alliance is also committed in that same document to help educate rights owners on how to protect their IP.

15. The Government's Digital Charter sets out the objectives of making the UK the safest place to be online and also the best place to start and grow a digital business, We welcome Government's stated aim in the Digital Charter to align "the same rights and expect the same behaviour online as we do offline" and

[11] https://www.gov.uk/government/news/search-engines-and-creative-industries-sign-anti-piracy-agreement

have already engaged with officials to demonstrate the problems faced by IP rights owners as well as the innovative ways in which Alliance members are engaged with consumers.

16. Alliance members support the need for the correct implementation and full application of existing rules relating to the online space, including those contained in the E-Commerce Directive and IPRED, to ensure the appropriate levels of protection. Online IP theft is clearly a significant and growing threat. New challenges emerge on an annual basis and the existing law often lacks the clarity required to protect against these challenges. The Government needs to look again at how it might create an enforcement regime that can react more quickly to these emerging threats without requiring primary legislation on every occasion.

17. The Alliance recognises the important role "safe harbour" plays in supporting the networks and technologies which underpin the online market but there is a distortion in licensing that arises from a misapplication of the safe harbour in European law. This has allowed a number of content service providers to benefit both directly and indirectly from the unauthorised use of creative content without the permission or remuneration of the rights holders - and has created a significant and growing gap between the value extracted from the increased use of premium content by certain platforms and the value that the creators and creative sectors are able to retain and invest. The Alliance supports the Government's commitment to continue to address the transfer of value from the creative industries and progress work on closing the value gap at European and domestic levels. In current EU discussions under the Digital Single Market, the issue of when online service providers might be liable for content uploaded by their users without the permission of rights holders and ensuring that proposals support creators without creating unnecessary burdens for businesses is ongoing.

18. The lack of enforcement of the transparency requirements in Art 5 of the EU E-Commerce Directive has led to illegal websites/platforms in practice running their online businesses in complete anonymity within the EU. The problem is exacerbated by the prevalence of anonymous online intermediaries (hosting providers, ad-brokers).

19. The importance of Article 11 of the EU Enforcement Directive being applied without prejudice to Article 8 (3) of Directive 2001/29/EC is underlined by the successful development and use of s97A CDPA in the UK. However in addressing the parallel provisions of the Copyright Directive and the Enforcement Directive (and the relevant of provisions within the E-Commerce Directive) there is a real lack of consistency over the ways in which the recognised importance of injunctive relief for right holders is established under in other EU member states.

20. Industry is working to protect IP rights in the digital world, allowing for the development of legitimate businesses and services which allow access to digital content. However, the scale of online infringement of IP rights is vast and represents both a significant and ongoing challenge for rights holders and creators

21. Legitimate businesses looking to utilise the opportunities provided by the growth of the digital economy are hindered by having to compete with those who infringe upon IP rights, and who do not properly contribute to creators and rights holders who fully invest in the creative ecosystem. In order to support development of the legitimate digital economy it is imperative that the law helps deter criminal activity in this area.

22. As noted by the European Commission, the understanding of liability for online intermediaries and platforms is core to how many businesses serving creative content function online. A number of rights holder groups have concerns around the functioning of "safe harbour" which plays an important role in supporting the networks and technologies which underpin the online market.

23. There is, in the view of these groups, a lack of clarity about the functions and purpose of safe harbour and that this is caused by the ambiguity of the appropriate definition of an intermediary.

Some rights holder groups state that this ambiguity has allowed a number of content service providers to benefit both directly and indirectly from the unauthorised use of creative content without the permission or remuneration of the rights holders - and has created a significant and growing gap between the value extracted from the increased use of premium content by certain platforms and the value that the creators and creative sectors are able to retain and invest.

Many are now calling for clarification to ensure that the safe harbour provisions should apply only to intermediaries that operate technological, passive and automated functions, and not to those who have knowledge or active control over the distribution of online content (some of which may not be licensed) but do not choose to implement measures to prevent circumvention of content protections.

24. However, even within the current regulations, the notice and take down regime is inefficient and ineffective. With the evolution of technology where unlawful content can be reposted and multiplied within seconds, the procedure has clear limitations. If service providers were to operate "notice and stay down", once a specific infringing file is notified to a service provider, that would go a long way to resolving the problem.

25. Regarding implementation of the EU Enforcement Directive, the UK Government took the view that national law already afforded right holders a high level of protection such that implementation of certain provisions (including under Article 11 IPRED) was unnecessary. Whilst this has caused uncertainty as to the courts' jurisdiction to make site blocking orders outside of the copyright context, the judiciary have so far proven willing to interpret national provisions in light of the Directive. In Cartier v Sky and Cartier v BT, Article 11 IPRED was successfully invoked along with national law provisions to permit issuance of an order against intermediaries, although the decision is under appeal. It is unsatisfactory that extensive litigation has been required to clarify the law in this area. As to the remedy itself, UK experience in the context of Article 8(3) of the Information Society Directive shows that the remedy is effective but that the evidence gathering process is both onerous and expensive.

About the Alliance

Established in 1998, the Alliance for Intellectual Property is a UK-based coalition of 20 organisations with an interest in ensuring intellectual property rights receive the protection they need and deserve. Our members include representatives of the audio visual, toy, music, games, business software, sports, brands, publishing, retailing and design industries.

The Alliance's overriding objective is to ensure that intellectual property ('IP') rights are valued and that a robust, efficient legislative and regulatory regime exists, which enables these rights to be properly protected.

The Alliance is also proactive in supporting the promotion of IP through educational and consumer awareness initiatives and encouraging the development of IP training for businesses and individuals seeking to develop, produce and trade goods, services and content.

Alliance Members

Anti-Copying in Design, Anti-Counterfeiting Group, Association of Authors' Agents, British Association of Picture Libraries and Agencies, British Association for Screen Entertainment, British Brands Group, BPI, British Toy and Hobby Association, Design and Artists Copyright Society, Educational Recording Agency, Entertainment Retailers Association, Film Distributors Association, Motion Picture Association, Premier League, Professional Publishers Association, Publishers Association, Publishers Licensing Society, UK Cinema Association, UK Interactive Entertainment

May 2018

Amazon – oral evidence (QQ 197-208)

Tuesday 8 January 2019

Watch the meeting

Members present: Lord Gilbert of Panteg (Chairman); Lord Allen of Kensington; Baroness Bertin; Baroness Bonham-Carter of Yarnbury; The Lord Bishop of Chelmsford; Lord Colville of Culross; Lord Goodlad; Lord Gordon of Strathblane; Baroness Kidron; Baroness McIntosh of Hudnall.

Evidence Session No. 22 Heard in Public Questions 197 - 208

Examination of witness

Lesley Smith, Director Public Policy, UK & Ireland, Amazon.

Q197 **The Chairman:** Good afternoon. May I welcome Lesley Smith from Amazon? She is our witness today in our House of Lords inquiry into the regulation of the internet, which is a fairly broad inquiry. We are very grateful to you, Ms Smith, for taking the time to come along to talk to the Committee. The session today will be available online and a transcript will also be taken, which you will have an opportunity to see. Thank you again for joining us. Perhaps, before I open up the meeting to Members of the Committee to ask questions, you could briefly introduce yourself and, in so doing, describe Amazon's main areas of UK business activity, and for each of them give us an indication of the relative size of the unit and its relative significance in the UK market, so that we have an understanding of the whole business.

Lesley Smith: I will try to. Thank you, Chairman, and thank you for the opportunity to meet with your Committee. We are a relatively young business in the UK. We have been in the UK for 20 years. Our ambition has not changed since the company was launched. We launched as an online bookstore in the States, but the ambition was very clear: to provide customers with a place where they could find anything they wanted online and to be the world's most customer-centric company. Those two things shape absolutely everything we do in our business strategy.

In the UK, we focus mainly on shopping and entertainment, on devices such as Kindles, Fire TV and Amazon Echo, and on services for businesses and sellers. Within that, there is Amazon Marketplace and things such as Kindle Direct Publishing and Amazon Web Services. The entertainment part is Prime Music and Prime Video. We have about 27,000 employees in the UK, which is rather different from the tech companies you have met so far. Obviously, we are a physical retailer, so we have lots of people moving physical things. Of those 27,000, about 19,000 are working in fulfilment services and customer services. The others are working in corporate services, in marketing and technology. We have four big tech development centres around the country working on innovations.

We think of the business as a whole as Amazon Marketplace and Amazon Retail. On our website, slightly over 50% of the items that are bought are not sold by us at all; they are sold by third party retailers through Amazon Marketplace. Those retailers include high street businesses and very small and very large businesses up and down the country. They are the seller of record. We do not own the goods at all. They can either fulfil directly from their own shops or premises and just sell online and fulfil it themselves, or they can put it in our warehouses and we offer Fulfilment by Amazon, so we deliver it and do the customer service and so on. That sometimes makes it much easier to achieve sales. We think those businesses are responsible for about 85,000 jobs and they did about £2.3 billion in exports in 2017, which are the last figures. We also have self-publishing with Kindle Direct Publishing. Of all the businesses that are enabled by Amazon in one way or another, from Marketplace businesses, to Kindle authors, to film production, to AWS, we think there are about 370,000 businesses that are in some way supported in their sales through Amazon.

I cannot talk about the relative size of AWS. It is an even newer business. We have had a cloud business since 2006 and it is a supplier of cloud services to businesses and enterprises of all sizes. That includes local authorities, charities and all sorts of organisations. Among our customers are BBC iPlayer, rather famously Netflix, and the *Financial Times.* Just Eat launched on Amazon. Citymapper launched on Amazon using Transport for London's data. Transport for London runs Journey Planner on Amazon Web Services. Cloud enables you to pay for what you use rather than having to invest in on-premises infrastructure. There is huge variety in the different services that are offered. There are thousands of different levels of service, from simple storage to all sorts of additional services such as running chatbots or using the kind of software that supports Alexa and Alexa apps and so on.

To give an example that will be familiar to most of you, UCAS—the Universities and Colleges Admissions Service—runs on AWS. It is a service where for most of the year people look for courses in architecture in Durham or sociology in Brighton, or whatever, in a fairly steady state, but in one week in August demand goes up because of A-level results, and it is absolutely critical that it can flex up and flex down when it needs to. It does not want to pay for that level of service throughout the year and it does not want to have redundancy throughout the year. It wants to be able to flex right up and to be completely resilient so that it is able to meet demand. Similarly, Transport for London on snow days or on a strike day will get five or six times the number of inquiries. It enables them to have that flexibility at much lower cost. New businesses, such as Monzo or Just Eat or Deliveroo, can enter their industry sector because one of their costs has been hugely reduced, not just by us but by the availability of cloud services from a big variety of players. It is a very competitive industry. The competition is pretty intense. There are new services all the time. We have reduced prices on AWS 68 times by simply changing the service, working with customers and looking at where we can make improvements.

The Chairman: Thank you. For clarity, and forgive me if I simplify it a little, I want to look at what you describe broadly as the retail side. I should declare an interest in that I am avid customer of Amazon and bought most of my Christmas on Amazon.

Lesley Smith: I am delighted to hear it, sir.

The Chairman: Roughly half of what you sell is sold by Amazon and roughly half is sold on behalf of others, whether you fulfil it or not.

Lesley Smith: I do not know if the value is roughly the same, but certainly in units just over half is Marketplace sellers and slightly under half is directly sold by Amazon.

The Chairman: And you fulfil some but not all of that Marketplace business.

Lesley Smith: It is partly to do with scale. Often, if it is a small business, it might decide to put some stuff on Amazon to see how it will go. If it has a fulfilment operation of its own, whether from its own warehouse, kitchen or shop, it will carry on doing that. Sometimes businesses want to scale up or to access international sales or are just growing and they will start saying, "Right, I am going to put it in Amazon's warehouses because it will go into Prime automatically and I can guarantee that it is much faster into the market".

The Chairman: If you look at what I see as the two main areas of your business, the retail side and the web services side, in the UK what is the rough relative size of those two units?

Lesley Smith: I honestly do not know. The slight difficulty is because we are a US-listed company, we report in the States. We do a consolidated report in the US and we report North America revenue and rest of world revenue. We break out AWS but we break it out globally and not by country. Within our American report we file a 10-K, which is a report for countries in which you have significant revenue, and our most recent revenue was £8.77 billion in 2017. However, that is all activity in the UK. I do not know what the break-out is of AWS versus anything else.

Q198 **Lord Gordon of Strathblane:** I imagine that somebody in your position sees their job as a two-way street, representing the company's interests to civic society here, and perhaps expressing the concerns of civic society about some aspects of the company's behaviour; to warn them in advance so that they can take anticipatory action.

Lesley Smith: Yes.

Lord Gordon of Strathblane: I imagine one of the issues you constantly have to mention is taxation, to follow on the point you made. I appreciate that it is an international company, et cetera, but I imagine from your point of view your job would be easier in dealing with civic society if Amazon paid a bit more tax, would it not?

Lesley Smith: I think it would be easier if there were a better understanding of how corporate taxation works internationally. Our worldwide tax rate, averaged over the last three years, has been more than 30%. We pay the corporate tax rate that most companies pay. I do not know where that fits in the averages, but it seems a fairly respectable rate. We are a relatively new business, so if you compare us in retail terms, and many people are wont to compare us with big well-known UK retailers, they have been in the UK for 100 years, and they have laid down and depreciated their infrastructure over 100 years. Ours has all been laid down very recently. In the last eight years we have invested £9.3 billion in the UK and, obviously, that has an impact on profitability in the short term. Our North American business is more profitable and our international business in the last few years has typically been unprofitable. That is not our long-term goal, but we are in a very deep investment phase. It goes without saying, but I will say it: we pay all the taxes that are due in every country in which we operate.

The other question is that Governments around the world and in Europe have been quite concerned about the phenomenon of international businesses that earn their income across borders. The issue is not whether they are paying enough; it is where they are paying and who is getting the share. The OECD has been working on how you divide that up. We think the OECD process is a good one. It is due to do some sort of report in 2020. The UK Government and other Governments would like that to be faster and we have a certain sympathy with that.

Lord Gordon of Strathblane: One solution that some people have touted is the idea of taxing you not on profits but on revenue.

Lesley Smith: I would question whether that is a solution. That is a very blunt instrument. First, we are already taxed on profitability so that tax is paid, but if the profits are low, the tax is compositely lower. If you are going to tax on revenue, you are in a situation where one company can ask, “Why are we as a company being presented with double taxation when other companies are not?” Also, people are looking at the technology sector as if it was all the same. We are a physical retailer so our margins reflect those of a physical retailer; they are very thin. There are other technology businesses which have much higher margins in the order of 40%. We have very thin margins and if you apply a revenue tax to an income stream on a very low margin, even though the level at which that revenue tax is set might in itself be low, if it is the same as the margin, it will be a 100% tax.

Lord Gordon of Strathblane: But you are still in a more favourable position than the high street retailers which have local authority taxes to pay.

Lesley Smith: So have we. We pay business rates just like anybody else.

Lord Gordon of Strathblane: Only in your warehouses presumably.

Lesley Smith: No, in every single building we have. There is no exemption. We pay them for our warehouses, for our head offices, for our technology development centres, for our delivery stations and for our lockers. We paid business rates on 94 sites last year.

Q199 **Baroness McIntosh of Hudnall:** What I want to ask you may be connected to this. I wanted to go back to what you were saying about the Amazon Marketplace retailers which are operating their own operations but using your platform. Could you give us some idea, first, of the spectrum of scale of those businesses? Are they mostly small and micro-businesses or do they include larger ones?

Lesley Smith: All sorts. I am trying to think of some names. House of Fraser was a seller. There are all sorts of different businesses. Black World Books sells on Marketplace. We ran an advertising campaign in support of small businesses on Marketplace in September/October-time. One of them is Shearer Candles. That is a relatively small business in Scotland. It sells through us, through Ocado, in John Lewis stores and it has its own stores. Originally, it had two or three stores, but it found it was able to build its brand online through Amazon, Fragrance Direct and some others, and it has now expanded its physical footprint and gone to five stores. It is difficult to think of a typical business because there are other online businesses that also sell through us. AO, the white goods retailer, sells through us as well. There is a huge variety in the businesses that sell on Amazon.

Baroness McIntosh of Hudnall: I saw the ads for the candle people, so that hit at least one customer.

Lesley Smith: Excellent.

Baroness McIntosh of Hudnall: That leads me to the second bit of what I wanted to ask you, which is the terms on which you operate with them. You were talking just now about your own margins being very thin. Generally speaking, if you have very thin margins, you need higher volume and you also need to do very tough deals with the people you are working with. Can you give us some idea of what the business arrangements are between you and the people on Amazon Marketplace?

Lesley Smith: I wish I had printed out the pages. It is very clear on Marketplace. We have Seller Central and if you go to our website, at the very bottom you can find "Sell on Amazon" and you follow the route and it gives you the fee rates for every different category. The fees are slightly different depending on the category you are selling in. Broadly, we have two categories of seller. You can either be an individual seller, so me selling my university textbooks or whatever, or you can be a professional seller if you are selling more than a certain volume, if it is your business. You pay a flat-rate monthly fee. I regret I did not bring the details with me so I cannot remember, but I think there is an additional very small fee per item. I cannot remember what the order is, but I am happy to send that to you, and that is set out by category so it is clear what the rates are. We aim to be as competitive as we possibly can. If you are simply listing, it is a transaction-related fee. If you are using Fulfilment by Amazon, we will charge you a fee that relates to storage and fulfilment.

The Chairman: May I come back? In response to Lord Gordon, you explained that the margins on your retail businesses are very thin. Are the margins on your web services similarly thin?

Lesley Smith: I do not know. I would have to come back to you. In everything we do, we aim to provide customers with the lowest possible prices. Every business in which we operate is highly competitive. There are lots and lots of cloud providers and lots and lots of retailers. The UK is among the most competitive retail environments in the world and among the best retail environments in the world. You have to operate on relatively thin margins. In cloud we are keen to drive down that cost. It is a business in which you have to do—and we have done—a lot of investment, and that investment has been relatively recent, but we are working with customers to drive down costs wherever we can. We operate on the lowest margins we practically can.

Q200 **Lord Goodlad:** May I change the subject to cloud, please? As more web services are moving to cloud, should cloud providers be regulated as an essential service?

Lesley Smith: May I take that in two parts? The answer as to whether they should be regulated is that they are regulated in many areas. I have a list somewhere. We are regulated as a processor under GDPR. We are a signatory to Cloud Infrastructure Providers in Europe. We have to observe codes of conduct. For example, the Financial Conduct Authority provided cloud guidance for financial services firms in coming on to the cloud. There are lots of layers of regulation in the UK, in Europe and internationally. There is the NIS directive on security. To that degree we already are.

You are asking a slightly separate question about being an essential service. Traditionally, you would think of an essential service as being one where there is a limited infrastructure controlled by a limited number of companies, without necessarily much variation. Electricity and water might fall into that kind of category, where you regulate because there is no competition, and you regulate because you regard it as something for which there are very limited substitutes. In the case of cloud, there is an enormous number of substitutes. Cloud is one way of providing infrastructure services, and the most obvious substitute is what most people currently have, which is on-premises infrastructure. They already have on-premises private servers or on-premises private clouds. There are layers and layers and a myriad of different services out there. There is massive opportunity for substitution. It is not essential. It is hard to say that we designate this kind of delivery as being essential when there are all these other alternatives.

Perhaps I am arguing myself around a corner. Should it be regulated because there are limited providers? There are not limited providers; there are thousands of providers and new ones all the time providing different kinds and levels of service. It seems to me that we have the regulatory tools. There is the CMA and all sorts of tools to protect competition, and to protect consumers and businesses using those services, but there is also incredibly fierce competition, and very rapid innovation and competition in that innovation, which should protect also consumers or businesses.

Lord Goodlad: In your view, is cloud a platform and how should cloud services be legally defined?

Lesley Smith: I would go back to the previous answer, which is I do not think it is a platform, because cloud is part of the myriad of infrastructure provision, and it can mean a lot of different things. Some of it is on premises, some is private cloud and some is public cloud. The connotations of the word "platform" are not helpful, because people think it means there is a kind of gate, and there is not. There are lots and lots of different ways of buying IT infrastructure services and you can buy lots of services from one business or you can buy a range of different parts of your provision from competing businesses. That does not feel to me like a platform.

Lord Goodlad: Thank you.

The Chairman: There are a range of options other than the cloud, but are you dominant in the cloud market?

Lesley Smith: No, because there is such enormous competition and speed. There is a difference between prevalence and dominance. One of the articles that the clerk helpfully sent to me yesterday refers to one of our competitors saying it had grown 89% in a year, without releasing any figures as to what its actual turnover was. An environment where you have new services and new providers all the time, huge amounts of investment and companies saying they are growing 89% in a year does not seem to me like an opportunity for anyone to be particularly dominant. There are lots of businesses fighting globally and innovating to offer new services and to bring new things to customers. We are a very long way from a situation in which you can say that anyone is dominant because the business is growing so much.

The Chairman: Do you have any sense of your market share of large public sector cloud contracts?

Lesley Smith: I honestly do not, but I am happy to come back to the Committee if I can find information on that.

The Chairman: Thank you. That would be useful.

Baroness McIntosh of Hudnall: Chairman, may I extend the question you have just asked because we have heard that Amazon does not regard itself as being dominant? Is it an aspiration to be dominant?

Lesley Smith: Amazon is a remarkably simple company in some respects in that we do not every year revisit our mission vision. We say, "Our mission is to be the place where you can find anything you want or need online". You do not need to be dominant to do that; you need to be good at what you are doing to do that and you need to work hard and find good partners. In talking about Marketplace, we did not set out to create a marketplace initially. We set out to be the place where you could find anything online. It is very difficult for one company to say, "We are going to provide one of everything". We simply could not do that. We spent a number of years looking at different ways of trying to find partners who would sell with us so that we could extend our offer to customers, several of which failed miserably. We launched shops online and they were not terribly successful. Marketplace is not separate from the rest of Amazon; it is completely integrated. We worked out that what consumers wanted to do was to search for the thing they want. If I search for blue shoes, I want to see everyone's blue shoes. I do not just want to see Amazon's blue shoes. I want to see blue shoes by Start-rite, Clarks, Geox and Adidas all in one place. That is how Marketplace works because it enables you, like a marketplace, to find everything. You do not need to be dominant to do that. You need to have really great business relationships and partners and find people who want to serve customers with really great products.

Q201 **The Lord Bishop of Chelmsford:** I take everything that you are saying, but you are perhaps painting a picture which is not entirely the picture that many of us see when we look at Amazon. Could we continue with the example of the blue shoes? Say I decided—and it is very unlikely—to buy, in my case, a pair of purple shoes, I would go on Amazon and look at all the purple shoes. Your people are also logging and are very good at logging what I look at and telling me, "If you like these purple shoes, you may like these red shoes". You might notice that one purple shoe is selling better than all the others, so what you do is produce your own Amazon basic version of the purple shoes.

Lesley Smith: No.

The Lord Bishop of Chelmsford: You do.

Lesley Smith: I think there is a bit of a conspiracy theory here.

The Lord Bishop of Chelmsford: Hang on a minute; let me finish. There is strong evidence of that, maybe not with shoes but with other products. Some businesses are very grateful for what you do. You provide a marketplace where they can sell their wares and nobody is suggesting that you are doing anything wrong. You are only doing with other products what Sainsbury's did with baked beans by producing their own-label baked beans. However, there is evidence to suggest that is holding back innovation and forcing some small businesses out of business and you are now achieving a dominance in certain areas. My question is: what sort of world do we want to live in? Even though you are so successful, do you also fear the world that is being created where you can get your Amazon version of everything?

Lesley Smith: First, let us go back to the question of dominance and then I will go back to the purple shoes as well and the individual products. On the question of dominance, 82% of UK retail is not online at all but is in physical retail. Only 18% is online. It is pretty difficult for anyone who is selling online in UK retail to be dominant. I do not see how anyone can do that. In our particular case we are a pretty small proportion of that. Our total sales for all activities, not just retailing but everything we do in the UK, was £8.7 billion in 2017.

The Lord Bishop of Chelmsford: But 18% is fantastic.

Lesley Smith: It is not just us.

The Lord Bishop of Chelmsford: Retailing 18% online is fantastic.

The Chairman: Could you address the Lord Bishop's question more specifically, which is about having intelligence from your users on products that are selling?

Lesley Smith: I will directly, but let me just finish with one sentence, because I would not want there to be a misapprehension on the record.

We are not even remotely at 18%. That 18% includes lots of retailers—Marks & Spencer, John Lewis, Sainsbury's, everybody. We are somewhere around 2% of UK retail.

The Lord Bishop of Chelmsford: That is eye-wateringly good and getting better.

Lesley Smith: We work very hard to have 2%. Tesco has 11%. On the purple shoes point, customers search for things, but our retail business does not see any data relating to our Marketplace business. We do not have that visibility. Marketplace sellers can see how their things are selling, but our marketing people cannot see the sales figures or any of the data that relates to a Marketplace seller. That is just not available to them. They can see the same as anyone else. There are loads and loads of independent businesses that track what is selling online. There is a company called CamelCamelCamel and you can go on to its website and see what is selling well on Amazon. We also display what is selling well on Amazon. Many Members of this House write books and they tell me from time to time they are delighted to see that their book is listed as a bestseller in ecclesiastical fiction, or whatever it might be. There are all sorts of things, including popular political books. I saw Andrew Adonis one day and his book was indeed, happily, top of whatever list it was that day. That information is available to everybody. You can see our bestseller lists in most categories.

Yes, we see what is selling well, but only as an outsider and not as an insider. Many years ago, I worked in physical retail before I worked in Amazon and we used to send store managers to look at our rivals to see what they had in their windows and what their prices were. We would say to people, "We need to match their prices and knock 50p off to make sure we are matching their prices", or you would say, "They have whatever it is in the green model; we need to get the green model too". That was 15 years ago. Every retailer watches what is selling well. Also, where we can, we offer our Marketplace sellers the same information as we offer ourselves. We have data on what people are searching for. You are right, if they are searching for purple shoes and we see the search information, we would tell our shoe buyers, "You need to get a lot more purple shoes". We would also tell our Marketplace sellers. We have a system called Nudge and in the category they are in we would see they had loads of blue shoes and we would send them nudges that say, "You might like to know that the most popular search in your shoe category at the moment is for purple shoes". That information is available to both sides, the retail side and the Marketplace side.

Baroness Bertin: Is the Chinese wall you speak about self-imposed as a result of business ethics?

Lesley Smith: Yes.

Baroness Bertin: Could there be a time when mission creep kicks in?

Lesley Smith: You go back to the fact that we absolutely have to be a trusted business. At the end of the day, people can choose to sell on Amazon or choose to sell elsewhere. There are hundreds upon hundreds of marketplaces. Very often parliamentarians think of two marketplaces but there are many different marketplaces—Alibaba, Wish, Depop, Shpock—in which they can sell. They can also sell through their own stores or online directly and so on. The most important thing for us is customer trust and that includes seller trust. I respect what you are saying. I know that some sellers think that because they sell something for a while and somebody else is competing with them, it is our fault because we have persuaded a competitor to come along. We simply have an open door. Anybody can look at what is selling well and say, "Do you know what? Spark plugs are selling really well. I should get out there and sell some spark plugs". That is not because we have special insight into how spark plugs are selling. On the question of whether you could start bleeding that information across, no, you could not, because that is about business ethics and maintaining seller trust. Those two parts of our business are separate to that degree.

The Chairman: We will move on now to another question area and Lord Allen.

Q202 **Lord Allen of Kensington:** I would like to talk about personal data. Should competition authorities consider the trade in personal data as a market in itself?

Lesley Smith: First, we do not sell personal data. I want to make that very clear. We do not make any personal or customer data available to anybody else. We have advertising on our site and we can direct information to a target group of customers, so the people who are searching for purple shoes or the people who are searching for garage doors, or whatever it is. That is the kind of data opportunity there is for advertisers with us and they can find a group of customers that are looking for those features, but we do not part with data in any way. We are obviously GDPR compliant, as you would expect. You can make a subject access request and see all the data we have. A lot of it is very visible so you can tell.

We provide recommendations, so if you have bought political books you will get served other political books. I get served, rather to my regret—my daughter browses from time to time and is keen on cats—a lot of stuff with cats on it. That is because those recommendations are based on search habits, but none of that data leaves us and goes anywhere. You can see on your own page the prompt that tells you, "People like you have bought things like this". If you go into your recommendations, you can also see underneath that there is a question every now and again, "Why am I seeing this? Why do I have this recommendation?" and you will click on it, and it will say, "Because you bought this and other people bought this". You can delete your browse history or previous recommendations if you want to.

Lord Allen of Kensington: I can see the benefits of personalisation and sending me the books that I like. Turning that on its head, what are the things that keep you awake at night on the negative side of that? What other issues, whether it is data theft or employees selling data, which your company has had an issue with, or whatever, should you be concerned about and would like to share with us in terms of your worry about data? You have seen hacking and theft and people selling data.

Lesley Smith: I do not think we have seen theft of people’s data—I hope—but I am happy to look into that.

Lord Allen of Kensington: In September 2018 you were investigating allegations about data being sold to third parties.

Lesley Smith: I will look into that. You are right: that would keep us awake at night.

Lord Allen of Kensington: As you get to the scale you get to and because of the fragility of data and the impact it would have on your business, I am just trying to understand the big data fears you would have and, more importantly, what you are doing about it as such a big player in this space. That is what I am trying to get at.

Lesley Smith: It is the same for any business. You do not have to be an online business to have a lot of data. Tesco Clubcard, Nectar and Visa have vast amounts of data. These days all businesses have a huge amount of data and all businesses have a duty to protect that to the greatest degree possible. We invest hugely in data security. We do a huge amount of training throughout the company. We are very restricted regarding access to data. There are a lot of levels of security as to who can see data. Everybody in the company who has any access to data does a lot of training about how you handle it and what you have access to. It is very highly restricted as to who gets access to any data. We spend enormous amounts of money on very sophisticated protection of all our networks. It is never-ending investment and a never-ending principle that you have to keep up to date constantly.

Q203 **Viscount Colville of Culross:** You say that you are not dominant but the public perception is that you are. This morning I read that you have 50% of online book sales in America. You talk about customer trust and its importance. There is concern that you could leverage your intermediary power to dominate the markets both vertically and horizontally, and a result of that would be that you could push down prices for products below their costs and restrict access to customers. Should you be concerned about that if you are worried about customer trust? Should the competition authorities be worried about that?

Lesley Smith: Yes, we worry about customer trust all the time. We are in lots of sectors, but we are broad rather than deep in most of those segments. I genuinely do not think there is any segment in which we are dominant. It does not seem to me that the competition authorities think that either. The competition authorities have a lot of tools to look at competition in every sector and at consumer benefit and at consumer protection in every sector. It is right they should use those tools. I do not think it is very different in the online world or the offline world. We have always had businesses that expand into related services or areas where they can see there is customer need for it.

You mentioned e-books. We started as a physical bookseller. We wanted to be much more than that and over time we eventually invented Kindle in 2007. It was not really about saying. “We want to put a piece of plastic into everybody’s hand and persuade them to read our plastic”, because we want people to read physical books as well. The idea involved the opportunity to allow people to download a book in 60 seconds wherever they were. We thought that was a fantastic innovation. It was exciting and thrilling and it kept people engaged with the book world.

We never believed it was going to switch people to reading e-books instead of physical books. We thought it was going to engage them with literature long term. Certainly our belief is that once you have an e-book reader of some sort—and it does not need to be a Kindle; it can be an app on your phone or your laptop; there are masses of different apps from different companies—and you are engaging with literature electronically or physically, the more you do it, the more you want to do it. You read a book on your Kindle; you recommend it to a friend; you join a book club, and so on and so forth. That is us going into a related area, if you like, but I do not think that is at all anti-competitive. It is learning about new services that you want to provide for your customers.

Similarly, we started with Kindle and went into Kindle Fire and Fire TV. All those things were the result of thinking about what our customers wanted. They used to buy DVDs from us and now they want to buy streaming video. We want to be able to provide those services. The CMA and everybody else have plenty of tools already that enable them to safeguard consumer interests and safeguard competition if somebody buys, say, another big competitor. If you buy a competitor, the CMA has adequate tools to deal with that. If you expand organically into another sector, it has tools to deal with that. I am not sure that it is different online from in the physical world.

Viscount Colville of Culross: There are stories of what Amazon has done to use its power through loss leaders. I have been reading about Diapers.com, which is obviously an American company. Apparently, you slashed nappy prices through the Amazon Mom program and absorbed the losses, and Diapers.com ultimately went out of business and Amazon Mom was able to pick up the customers. There are other stories like that, so people are concerned.

Lesley Smith: I do not know anything about the Diapers.com story, but there are stories in retail all the time about how one company has reduced its prices. The supermarkets are much more caught in those stories than we are most of the time. I do not know about that particular case, but, yes, we have some products that we will try to offer at as low a margin as we can because we want to attract customers. I think retailing has always been like that. If you go into any supermarket in the land, you will see a gondola end full of products that are at a much lower price, which draws you into the rest of that aisle, because you think, "Good, red wine is cheap; I'll go and look at the rest of their wine, too". That is just retailing.

I cannot answer that particular question, but in general we seek to be competitive. We want to be competitive and we want to attract people. I do not think for a second that we have any interest in taking out competitors. That is not how it works. You want to have enough of a range of products so that customers come back to you and continue to shop with you. We really do not spend our time thinking about the competition. We spend our time thinking about customers and how they shop. If we spend our time thinking about the competition, we are failing to think about what we need to be doing for customers. We are failing to look at the things our customers are looking for and at how we are going to get more of the things that our customers want to buy and at how we arrange ourselves so that we can offer those quickly, or offer a good range of choices, or offer them things at the right prices. Let us find more partners who can provide the things our customers want to buy. We are not the kind of company that spends its time thinking, "Let's look at who else is in this business", and worrying about the competition. Right at the top of the company, the first day you do your training when you are inducted into Amazon, people say, "Our job is to worry about the customer; not to worry about the competition".

Baroness McIntosh of Hudnall: You have talked about the customer and you have talked about the competition but what you have not talked about is the creators. For example, in the model of bookselling that Amazon has so successfully marketed—and, hands up, I have a Kindle and I buy books that way and it is very useful and convenient to be able to do that—I sometimes think, "What is the person who wrote this book getting out of this?" As the retailer, how much time do you spend thinking about the people who actually create the content, not just the books but the other things that you sell, without whom you would not have anything to sell? How much time do you spend making sure that the deal you get for them is good enough that you can provide a really hot deal for your customers about whom you are most preoccupied?

Lesley Smith: The answer is "a lot". Interestingly, we meet the Society of Authors quite regularly because from time to time it has the same concerns that you have suggested. We meet with the Publishers Association. We meet all our buyers and with everybody who provides products in different guises. The book team will meet people in the book industry and the fashion team will meet people in the fashion industry, and so on. Again, it is not in our interest to make things difficult for our suppliers. We never want to do that. We want to be in an environment where they can sell more and earn more of a living. We believe that that has been extremely successful in the book segment in particular. There are more books being published every year, partly because the routes to self-publishing have become available so many more authors can publish either online or publish through CreateSpace and print books on demand, and earn a living at their craft. That is very new and it is a huge opportunity.

The book industry has certainly changed and it has changed not just because of us but because of the fact that supermarkets and all sorts of different places sell books. There are more places you can buy books than there ever have been at any time.

Baroness McIntosh of Hudnall: It is not just books, is it?

Lesley Smith: No, it is not.

Baroness McIntosh of Hudnall: The music industry has changed partly because of your interventions. I do not mean this to sound like an accusation. I am simply saying it is a fact that, as a company, you are now intervening in the creation of content so that other providers have you as a competitor not just through what you market but through what you create.

Lesley Smith: For all those industries, the internet, and not just Amazon, has changed everything. Music, creative content and all sorts of things have changed a lot because the internet has made things much more available and accessible. Having a secure way of selling books that is resilient to piracy has protected the book industry in a way that is much more difficult for the music industry. Being able to encrypt books and protect them and sell them at a price that is sufficiently attractive that people would buy them rather than steal them is a very positive thing. There is always a tension. If you are an author, you want to secure the best price for every product, but you also want to sell a lot of product and you want your book to be widely known. That is a negotiation you would have with anyone selling anything. You would have to work out the elasticity and the trade-off and how best they can maximise their revenue, and we want to support people in maximising their revenue.

I keep going back to the book example. We promote the author and the literature. We do not promote just e-books or just print books. I was reading a book by Kate Moore called "The Radium Girls" over Christmas, which is utterly brilliant. You will find the author's name and the audio book, the print book, the hard-backed book and the e-book side by side. We are very neutral about how you buy it. We do not mind. We are promoting it so that you buy it and promoting availability. We have an authors' page behind it. You can blog on the site and promote your book in any way you can. We urge publishers to support their authors in doing that. We want that to work and we want that to be true for all our suppliers. That is also true for creative content. Yes, we have lots of people who are making creative content now for Prime Video or who are marketing their music through Prime Music. We believe that the same thing holds true and that being available to customers on an international basis is a huge opportunity. It is a fantastic opportunity for getting people's names known and making content available. It is not only Amazon; there are plenty of other competing sites that provide music or video content or books.

The Chairman: I think you have made this point and we appreciate it, but time is pressing and we need to move on at a bit of a pace. Lord Gordon.

Q204 **Lord Gordon of Strathblane:** In answering Lord Colville earlier, you mentioned that the CMA has quite a range of tools at its disposal in dealing with mergers. One tool it does not have, which it has offline in the case of media, is a public interest test. Do you think that a public interest test might, with profit, be brought into its weaponry?

Lesley Smith: Do you mean for retail?

Lord Gordon of Strathblane: No, for the transfer of data. I am not saying this directly affects Amazon. I am just asking it as a question.

Lesley Smith: I am sorry, I have not thought about it in that way. There are no successful companies that are not using lots of data one way or another.

Lord Gordon of Strathblane: I am talking about the transfer of data from one company to another, which you have said you do not do, so I am excluding you from it.

Lesley Smith: You mean selling data. I am not entirely certain I can answer that question. There are companies whose business model is around selling data. We are not one of them. You already have rules within the GDPR that protect consumers' private data. Whether you need the CMA to have a role in that, if I am honest, I have not considered that.

Lord Gordon of Strathblane: If we move on to a different aspect of your activities, Amazon seems to expand horizontally quite a lot. It may be by accident or by some grand plan that nobody knows about. One area you have now gone into to quite an extent is video on demand. Some people are worried that at the younger end of the age spectrum, video on demand has almost replaced broadcasting as the means by which people watch the programmes they like to watch, or television or films that they want to watch. First, do you think the provision of video on demand should be subject to the same degree of regulation as broadcasting?

Lesley Smith: It largely is. There used to be ATVOD and ATVOD became part of Ofcom. There is a slight misperception about whether it is regulated or not. Ofcom applies very similar standards to video as it does to broadcasting.

For our part, we provide video on demand through Prime Video. There are very easy parental controls on that site. If you have an Amazon Fire TV Stick, you can enable parental controls from day one, so it is very clear. If you go back to the years before streaming, and even before digital television, the only control people had was the watershed, so the assumption was that children would be protected by being in bed by 9 o'clock. I would that were true in my house. Now we have much more sophisticated tools and we provide really simple parental control PINs. We do that not only on Fire TVs but on devices. We have a product called Kindle Fire for Kids where there is no in-app purchasing and no advertising. Parents can control how long it is on for and they can restrict it so many times a day. They can say, "You can only watch videos after you have read so much on your e-book‟, or whatever it is. Parents can have a high degree of control.

Lord Gordon of Strathblane: Following a recent speech by Sharon White of Ofcom, I gather the Government are consulting on the equivalent of EPG prominence on digital services. How would Amazon respond?

Lesley Smith: I am aware of that. The answer is that we are still thinking about it. I am glad she is doing a consultation on it because there is a lot to be discussed. You have to think about the different ways in which people consume media. Would you mandate prominence on a mobile phone? I do not know. She has some difficult things to think about in how you make that work. For my part, my interface is my Fire TV or my Fire TV Stick, but when you go into my self-controlled EPG, at the moment the first thing it has is BBC iPlayer, then All 4 and then "The Marvellous Mrs Maisel". I think it is a good debate to have and we welcome the fact that Ofcom is doing a consultation. It is complicated because you have an awful lot of consumer-enabled choices and how you do that and ensure that visibility for public service content is still there.

Lord Gordon of Strathblane: You would accept that it is desirable that there is high visibility for public service content.

Lesley Smith: Yes, I would. I do not know how you answer that but in principle, yes. Have we thought hard about our response and made a response yet? No, we have not.

Baroness Bonham-Carter of Yarnbury: To be honest, I think my question has been covered.

The Chairman: Baroness Bertin.

Q205 **Baroness Bertin:** Could we talk a little about design? You mentioned just now about interfaces. How much time and effort do you spend on the design of your interfaces, because, presumably, that is key? Some people in evidence to this Committee have described it as "surveillance capitalism" using various phrases such as that. I would like you to expand a little more on that.

Lesley Smith: I have never heard the phrase "surveillance capitalism" before and I am not entirely certain what it means either.

Baroness Bertin: You can ask the professors from Cambridge what it means.

Lesley Smith: I will look it up. We spend a huge amount of time on it. Our job is to ensure that we make life easy for customers. I keep going back to online and offline examples. If you were designing a physical shop, you would have test stores. You might say, "I have a chain of retailers. I want to change how people see fashion because they are not seeing the right clothes, so I am going to have three test stores, and in this one I will put hats in the front, in this one I will put boots in the front and in this one I will put handbags at the back", and see what changes in how customers find stuff. That is what physical retailers used to do and, for all I know, still do. They have test stores and pilots. It is hard to navigate a little square and find all the things you want. It is harder still when you are doing it on an app. We spend a lot of time thinking, "How can we make this easy for customers? How can we design this so it becomes as intuitive as walking around a shop and knowing where to find things in a department store?" We spend a lot of time on that. We test stuff and we pilot stuff and we use our staff to test stuff, as any retailer does.

Baroness Bertin: Presumably, that design is based on customer data and on algorithms.

Lesley Smith: Yes.

Baroness Bertin: We have spoken quite a bit in this Committee about the accountability and transparency of algorithms. Do you have a view on that?

Lesley Smith: The word "algorithm" has a bit of mystique attached to it, but algorithms do maths. It is exactly the same as old-fashioned retailers counting footfall data and working out that more people came on Sunday afternoons than came on Tuesday afternoons so they began to open on Sundays because people were free, or that a product sells better if you put it here rather than put it there. All those things are algorithms. We have more data now and we can compute it much more efficiently, but all you are doing is looking at what customers do and seeing how you can help them. We would use an algorithm to predict how many blue shirts we will sell this year. That is based on how many blue shirts we sold last year, what is in fashion this year and all sorts of different things.

Baroness Bertin: Sure, but with everything that has gone on over the last year, rightly or wrongly, there is a growing sense of public mistrust in the use of data. We know all that. You talk about business ethics, but would it not be of interest to be more transparent or is that not part of the debate at all within Amazon?

Lesley Smith: I think we try to be quite transparent. In our terms and conditions there is a little bit that says how we use data and a bit on our privacy policy, which explains to people how data is used and how we do stuff. No retailer publishes its pricing policy because that is commercially sensitive, so most retailers watch that all the time and say, "So-and-so is doing that a different way; I wonder why they are doing that?" They are doing that because they have observed their customers and have thought hard about what they are doing. I am really glad there is a Centre for Data Ethics and Innovation because, in public conversation, it is good to demystify some of these things and say, "This is not sinister". People have always watched what customers want and what customers do, in order to be good at their job, and to try to serve them with the things they want as efficiently as possible, and not to waste their time.

Again, when I was in physical retail, one of the things you would track is how many customers came into your store and walked out without talking to anyone, because that was a failure to engage. If the customer did not find anything they were interested in in your store and they only came in to get out of the cold, you were not doing something right. That is the same for us. Not just retailers but everybody online is measuring how long a viewer or customer, or whoever they are, spent with them before they left. On a Kindle, did they read 20 pages or 300 pages? Did they chuck this book away after the first five pages? In a store, did they spend 20 minutes or half an hour? All those things are measured and computed by algorithms. Perhaps not us specifically but users of data should talk a little more about how they use it, because explaining what we are doing might make it seem a little less sinister.

Baroness Bertin: I think you are on to something there, to be honest. I have a final question. I accept what you say that you only have 2% of the market and you are not market dominant and all the rest of it, but companies such as Amazon are changing the way society acts and behaves. As a company, how much time do you spend worrying about that, if indeed you do? For example, the high streets are closing and all the rest of it, and I would like your views on that.

Lesley Smith: I could never answer the "how much time?" question because I do not measure how much time is spent.

Baroness Bertin: Sure, but is there an emphasis on it or is it even considered?

Lesley Smith: We talk about the high street a lot, partly because people ask us about it a lot. We are on the high street in some cases. We have Whole Foods, which is a very small operation in the UK, but we have some Whole Foods stores and some book stores in the States and Amazon Go in the States. Those are very tiny operations that we are thinking about. Yes, we think about that. If you go back to Marketplace, many of the Marketplace businesses that sell on Amazon also have high street premises and they are thinking about their businesses. Nobody went out to say, "We must take people away from the high street". The internet exists and it provides a way to provide opportunities for customers.

Q206 **The Chairman:** I think what Baroness Bertin is asking is: do you worry about what is happening in the high street?

Lesley Smith: I think everybody worries about it. Everyone who lives in the country thinks about it.

The Chairman: As a corporation, do you worry about the high street?

Lesley Smith: Yes. In various parts of the country, we are a part of the local community. We have tens of thousands of staff who are in the communities around our fulfilment centres or other parts of our business. We are part of various local business development areas and business development groups. We are part of that debate about how we can strengthen the high street and what we can do. Some of that is about change of use and much more flexibility in how space is zoned and arranged. We take part in that debate as much as anybody else. I do not pretend to have any great expertise because that is not a place we do business.

I met the Commons Housing, Communities and Local Government Select Committee in the future of the high street debate just before Christmas. It was having that debate about business rates and retail premises and how you change the high street to ensure that people use a whole range of different services. We help with that to some degree in that we have 16,000 Click and Collect locations. Every post office in the country has Click and Collect and that drives businesses. We do that with other retailers. The Co-op has Click and Collect locations. We have lockers in stores and shopping centre car parks. The reason retailers want to have Amazon lockers is that it drives footfall into their stores, and we are very happy to work with them to do that.

The Chairman: I have a quick and fairly precise question on interfaces, which we talked about a moment ago. If I ask Alexa as one of your interfaces at home to order my favourite red wine and it is available both from Amazon and from Marketplace at the same price with free delivery, how does Alexa choose?

Lesley Smith: On the basis of your preferences. It is what you ordered last. On my Alexa I have AmazonFresh and Ocado and I have both apps enabled. If I say, "Add this to my shopping list", she will say, "Which one?" and offer me either the Ocado one or the AmazonFresh one.

The Chairman: If I ask her to find me a product that I have not bought before and it is available both from you and from an independent retailer, what would she do?

Lesley Smith: She would say, "I have found the following things", and she would put it in your shopping list. It is the same as a physical search in that it will find the product that most closely matches your search.

The Chairman: So it would never default straight to the Amazon option. If there is more than one option, it will give you those options.

Lesley Smith: It will give you those options. I see mine. I have an Echo Show, which I recommend to you, which is the one with the little screen, and it will say, "I have found the following products that match your request".

The Chairman: I do not have a screen on mine.

Lesley Smith: I do not know what they cost these days but I could make you a bargain offer. Mine will show me the five or six items that match my search and I pick one, or it will put the list in and I will select it on the app.

The Chairman: We will have a couple of interventions and then we will move on to the final question. Lord Colville.

Viscount Colville of Culross: You said that customers and customer needs come first. I am looking forward to where this will all go. I understand that in 2012 in America you filed the patent for anticipatory package shipping, which is shipping product before the person even knows they want it. It was slightly mind blowing. Is that going anywhere? Is that being rolled out?

Lesley Smith: We file a lot of patents and some develop and some do not. I am dimly conscious of that one. We file a lot of patents and some of them come to something and some of them do not.

Viscount Colville of Culross: Do you expect anticipatory package shipping to be coming our way?

Lesley Smith: I have very little idea. I am very sorry.

Baroness Bonham-Carter of Yarnbury: You have mentioned Whole Foods a couple of times in response to supporting the high street. What is your plan for Whole Foods?

Lesley Smith: We would like Whole Foods to be great and customers to love it.

Baroness Bonham-Carter of Yarnbury: And for it to remain in a physical building.

Lesley Smith: Yes, yes, absolutely.

The Chairman: The final question area is from Baroness Kidron.

Q207 **Baroness Kidron:** I think my colleagues have covered a lot of this and you have answered very fully. May I ask you a very general question on what you understand by the words "ethical by design"? A lot of people have mentioned that in the course of our inquiry. Would you answer that and then I have some more specific questions that I would like to ask?

Lesley Smith: I suppose it goes back to the fact that we want to ensure in everything we do that we are offering customers, to the best of our endeavour, what they want, and protecting their interests. We do not want ever to put customers at risk. We are predominantly an adult site, entirely an adult site in fact, but in as far as we produce products for children, such as Kindle Fire for Kids, we have spent a lot of time thinking about how children use things. We did focus groups and asked, "What are the things parents worry about or what are parents concerned about in this product?" Parents are concerned about kids inadvertently buying stuff on apps—in-app pop-up advertising. They are concerned about inappropriate content and kids being too long on screen. We said, "Let's work out the things we can do to fix those things". Parents can manage time limits. When my daughter had a Kindle Fire for Kids, she was allowed 20 minutes a day and an hour at weekends. She was really cross about it, but it was very easy to set up with a password. I set it up so that there was no advertising and no pop-ups and it was a very restricted browsing experience. In that particular case, it was thinking about the product, but it is different product to product. You ask, "What are the things people are concerned about in this product space? What risks are they concerned about and how can we best safeguard that?"

When the Minister answered this question, she said that you want "an environment where companies are incentivised and their motives and algorithms are aligned with the public good and higher ethical standards". I agree with that, but companies that know they succeed or fail on the basis of customer trust are already highly incentivised. If we forfeit customer trust, that is the game over. I have to do customer awareness training and code of practice training, which is renewed every year, and the thing that comes up first is, "What is Amazon's most precious asset?" It is not AWS or Marketplace or shedloads of data; it is customer trust.

Baroness Kidron: I am curious about that because there is also a tension between convenience and trust. In the digital sphere, a lot of people might find themselves doing something very convenient that perhaps they do not trust. Do you ever look at that?

Lesley Smith: We have lots of measures of customer trust. There are independent measures, our own measures and we do independent polling. We spend a lot of time measuring customer trust. The most obvious thing is whether people come back. Yes, we absolutely seek to offer convenience, but we seek to do it in a way that is transparent, where people understand what we are doing. One of the things I spend the most time explaining is Marketplace and how it operates. I welcome the opportunity to do that.

We had a group of sellers who met Ministers and MPs and we try to get more and more of our sellers to engage with what we are doing so that they are able to advocate to their colleagues. We want to build trust with them. Possibly that communication is a bit overdue and we are working harder at that communication to ensure that sellers have greater confidence in how we look after them and how we operate. We provide an awful lot of information to them and we want to communicate that more effectively. We spend a lot of time worrying about customer trust.

Baroness Kidron: In the course of the afternoon, you have given a very good account of the similarities between Amazon and retail in general, but is not the difference that you are in people's homes, in their bedrooms, in their pockets, and you are integrated into their lives, and that is part of the success but perhaps part of the problem area?

Lesley Smith: It is something customers choose but they do not just choose Amazon. Many of you will have a mobile phone and on it you will have various apps and you will look at social media and look at us. When I am in the canteen at work and I see someone with a nice jumper, I might say, "Where did you get that?" I was speaking to somebody at Christmas and I said, "That's really nice; where did you get that?" and she said, "Oh, Instagram". Yes, in that case it is convenient, but she is also in a slightly different market segment than me—she was 20 years younger—and it had not occurred to me to shop on Instagram. All those things are convenient, but they are also highly competitive, so the safeguard is there are lots of ways of doing things and lots of different choices. People are not sitting at home with Amazon as their only option. They have a great many choices.

Baroness Kidron: Forgive me if you thought I was accusing Amazon; I do not think I was. The competition that you describe is perhaps experienced by the consumer in a slightly different way because you all compete against the one poor us. Back to this ethical issue, where perhaps my colleagues Baroness Bertin and Lord Colville were going in talking about anticipatory purchasing and so on is the fact that we have a new world order in which Echo hears our voice. We know that the emotions of a voice are much more available than the emotions available through ordering something in that way. There are new forms of interaction in this space and these are the things that people concern themselves with. With opportunity comes new risk and that is the way that we have been looking at it. I do not think anyone wants to get rid of Amazon or, indeed, the internet.

Lesley Smith: I am relieved by both of those things. You are right, of course, that as society changes and the way we do things changes, there are phases of excitement and then it becomes normalised. People change their behaviour in that excitement phase and then it calms down. To go back to the anticipatory purchases point, we have something called a Dash Button, which you can put by the washing machine and when you run out of washing powder, you press a button to say, "Buy me the same thing again". We spend some time thinking about how we can engineer that convenience more effectively. I do not know about anticipatory purchases, but I suppose if you are a regular purchaser of dog food and your dog always eats at the same rate, you might be able to anticipate, “We will deliver that person’s dog food sale or return every three months”. I have no real idea how it might work, but, hypothetically, it could be like that.

What happens is that people get very enthusiastic about something because it is new, but it is no longer unique after a while and there will be lots of choice, and people rebalance. “It was very exciting buying it this way. Now I am going to go back to buying it that way”, or, “I am going to carry on and some of it I will buy this way and some that way”. I buy e-books and I buy physical books. I am lucky enough to have a physical bookstore at the end of my street and I buy physical books as presents, partly because it is there and partly because the touch and feel is there, and that is fantastic. I also love being able to download it on the phone because instant gratification is nice.

Baroness Kidron: Is it not the case that the Dash Button has surge pricing?

Lesley Smith: No.

Baroness Kidron: Categorically not?

Lesley Smith: No, it is the same price as you would get on the website. There are lots of little buttons. There are buttons for all sorts of different things—cat food, dog food, washing-up liquid, loo paper, whatever—and it replenishes what you typically order on your website order.

Q208 **The Chairman:** Your mantra has been the mantra of any successful retailer, which is the customer is king and that your objective is to serve your customers and have their trust. Do you see serving your customers and retaining the trust of your customers as doing the right thing for society?

Lesley Smith: Part of it, yes.

The Chairman: By doing the right thing for your customers, you are doing the right thing for society.

Lesley Smith: Yes, but it is not the only way. Doing the right thing for society is a lot more than that. You mentioned Alexa. We started off with developing a product, Alexa. At the time you are developing a product, you think, “What is the potential of this product?” Who knows? The thinking was that this would be a great interface for a smart home, which is one of the things we were looking at at the beginning. The smart home started with people saying, “It would be really brilliant if you could turn your lightbulbs on from your mobile phone”, and it turns out that it is not that brilliant. It is quite easy to turn your lights on and off and getting out your mobile phone, putting in a passcode and doing it is not that convenient.

However, the next step was that the idea that it would be convenient to be able to say, “Alexa, turn the lights on”, or, “Alexa, switch on Radio 4”, or, “Alexa, set a three-minute timer for my egg”. All those things are convenient and quite fun and they make life easier. For me, they are not necessary but they are nice to have. When my mother was alive, what I really wanted to do, if it had existed, was to set it up to say, “Remind my mum every three hours to make a cup of tea” because she won’t remember, or to be able to leave messages on it. I have a facility on mine with my brother where I can just say, "Drop in on Donald", and it will ask him if he is there.

We had some ideas about what we wanted to do with it. We wanted to be able to offer music and all the things that we offer through other sites and give people the opportunity to use voice for browsing rather than a screen, but we did not have a clear idea of all the things you could do. We worked a bit with the RNIB and its American equivalent to think about, "What are the things you could do with this to enable people to live their lives more easily?" The RNIB is a fairly obvious opportunity for people to use it. It is further developed in the US than it is here because it has been there longer. They have worked with a number of charities to look at services that can be developed for particular groups in society who want to develop skills. We have supported them in how they do that. We have sat down with them and said, "Tell us what their needs are and how we can help you to do that". It is sort of early days and we are feeling our way in asking how we can do that. We have a development centre in Cambridge where a lot of the Alexa voice technology is developed and it has sat down with a number of charities, with educational groups.

The Chairman: Is that a global development centre?

Lesley Smith: Yes. All our development centres do stuff for our global business. If the Committee wanted to come and see that or find out more about it, we would be very happy to arrange that.

Baroness Kidron: We are very used to talking about the big five or the big seven, if you include China and so on, but it is very clear that everybody is moving towards the same place, as Prime does content and Instagram does shopping, et cetera. Do you think we are on the verge of seeing something quite huge as the big five battle for or become the same thing?

Lesley Smith: What do you mean by the big five?

Baroness Kidron: The big companies, I guess Google and you and Facebook and so on.

Lesley Smith: We are all very different.

Baroness Kidron: But you are starting to do more of the same things. There is gradually more and more overlap.

The Chairman: As you demonstrated, Instagram are getting into shopping.

Lesley Smith: That is true.

Baroness Kidron: Original programming is now done through Amazon, Apple, Love. Is this the future?

Lesley Smith: That falls into the basket of we do not think about the competition; we think about what we are doing.

Baroness Kidron: Thank you.

The Chairman: Lesley Smith, thank you very much for your evidence. It has been very useful. You have offered to write to us on a couple of things to follow through, but the clerk and you can sort that out. Thank you very much indeed for your time.

Professor Leighton Andrews, Cardiff Business School – written evidence (IRN0041)

Submission to the House of Lords Select Committee on Communications: The Internet: To Regulate or Not To Regulate?

1. I very much welcome the Inquiry announced by the Committee. I will keep my submission brief. In summary:

    a. Potentially the most valuable outcome of the Committee's inquiry could be to change the language around the question of the regulation of the Internet, re-setting the problem from 'The Internet: To Regulate or Not To Regulate?' to 'whether a new regulatory framework for the Internet is necessary' as outlined in the Committee's Call for Evidence. The Internet – and the World Wide Web -operates within a framework of regulation, self-regulation, co-regulation, industry codes, statutory guidance and so on: it is disappointing when people, including existing regulators, reduce the issues to a binary choice between regulation and censorship.

    b. The regulation of the Internet engages several regulators and advisory bodies, as the Call for Evidence indicates. The Internet Commission has suggested in its evidence (IRN004) that in the UK, as many as 12 regulators are involved in content regulation or online interaction. A patchwork of regulation may always be necessary, rather than a single over-arching regulator, but care must be taken to ensure that there is effective coordination between them and between them and international regulators, particularly if Brexit happens.

    c. We need to consider the possibility **of 'ex ante' regulation in respect of online dominance** in specific markets such as search and social media.

Regulation is not a binary choice.

2. It was profoundly disturbing to read statements by the chief executive of OFCOM at the Royal Television Society conference last September that while she believed that Facebook and Google were media companies she didn't 'think regulation is the answer because I think it is really hard to navigate the boundary between regulation and censorship of the internet.' She repeated this at the House of Commons Select Committee on Digital, Culture, Media and Sport in October.

3. This language is curious: it is very much the language of the internet platforms themselves. Ofcom regulates the BBC, ITV, Channel Four and S4C amongst others – no-one speaks of them being censored. In any case, Parliament has legislated to regulate social media platforms. The 2017 Digital Economy Act, to take one example, puts a duty on the

Secretary of State to draw up a code of conduct giving guidance to social media platforms in respect of online abuse. While the code is not mandatory, its creation effectively provides space for social sanction to companies which do not comply with it. Parliament has therefore brought social media platforms within the context of a form of regulation.

4. Other regulators have taken action in respect of the Internet Intermediaries. For example, the Information Commissioner held an eighteen-month long investigation into the issue of data-sharing between Facebook and WhatsApp which has resulted in WhatsApp signing an 'undertaking' wherein they have given a public commitment not to share personal data with Facebook until they can do so in compliance with the upcoming General Data Protection Regulation: https://iconewsblog.org.uk/2018/03/14/whatsapp-signs-public-commitment/. Meanwhile, the European Commission has taken action against Internet intermediaries, levying large fines on Facebook and Google.

5. In any case, the Internet is subject to regulation in a number of ways from its underlying hardware and networks to the software and applications which govern our day-to-day interactions. Others have far more expertise in this field and I shall leave that to them.

Regulation needs co-ordination

6. Regulation of social media is something of a patchwork, drawing on legislation in both the UK and EU. This is understandable, as regulation and technology has evolved over time. Google was incorporated less than 20 years ago, and Facebook and Twitter are less than fifteen years old. Smartphones, which have driven social media take-up, are really only a decade old. In some areas, such as the issues that have arisen in respect of Cambridge Analytica, AggregateIQ and Facebook, several regulators have a role. Regulators do meet and talk with one another, but some of the challenges now being faced may require more strenuous coordination. The Electoral Commission has raised questions over whether the powers that it has are adequate to address the new social media environment. New powers have been tabled for the Information Commissioner in the Data Protection Bill.

7. Given the power and dominance of two of the social media platforms in particular, Facebook and Google, it is questionable whether the regulatory armoury is sufficient. There is a specific problem for competition regulators: as the OECD has pointed out, it is difficult to use traditional competition policy tests, such as market definition, in the presence of 'zero' prices, where customers are essentially paying through their attention and their data. Social media and search algorithms are not transparent, and it is known that many consumers are not aware that their Facebook News Feed, for example, is algorithmically determined: there should be greater transparency in respect of algorithms, overseen by an appropriate regulator.

8. If Brexit happens, then there will be an enhanced need for cooperation and coordination with European Member State regulators and the European Commission. Given the extraordinary dominance in certain markets of Facebook and Google in particular, the UK will need to consider whether existing legislative powers are sufficient, particularly in respect of competition.

Ex-Ante regulation in respect of online dominance in certain markets.

9. Facebook and Google may be media companies or publishers, but they are more than media companies. They are advertising engines, data controllers, information service providers and algorithm developers and they are moving into a variety of new fields such as artificial intelligence, virtual or augmented reality, leveraging the revenues they are earning from advertising. Their corporate power is unprecedented. They have purchased early-stage ventures which might have turned out to threaten their position and their dominance risks damaging innovation. In their main fields, they are arguably now natural monopolies. The role of network effects and economies of scale driven by Big Data consolidates and concentrates their power as first-movers. The entry costs for new suppliers are so high as to be prohibitive. Their ability to imitate and replicate at low cost the new services offered by competitors reduces the effects of competition. It is difficult for consumers to switch or exit when in the case of Facebook, most of their friends may be on the platform, and in the case of Google, its dominance of data makes it difficult for any other search engine to approach the quality of service it provides. Cross-platform sharing of data within a group of companies intensifies their dominance and is only partially addressed by post-hoc fines, such as those handed out to Facebook and Google by the EU's Competition Directorate. Both have a gatekeeper or bottleneck effect - strategic control of the gateway to consumers, particularly important in the media markets, for advertisers, app developers and others.

10. They are arguably now performing a utility function. Indeed, Mark Zuckerberg has long spoken of Facebook as 'a social utility' or 'social infrastructure'. In the past, Parliament has regulated to control such monopoly power. For example, the 1984 Telecommunications Act, introduced when BT was privatized, recognized the danger of such a dominant player being able to exert anti-competitive power and put in place a strong regulatory framework. The situation of Facebook and Google is different, but they are dominant in their spheres and have significant market power. Their potential for exploitation by hostile state actors, as we have seen in both the US Presidential election and in the UK's EU referendum, means that they should be seen as critical social infrastructure.

11. A new framework of regulation should be established. One such framework was outlined by former senior Ofcom regulator Robin Foster in 2012. In a report for the Reuters' Institute for the Study of Journalism entitled *News Plurality in a Digital World*, he called for 'statutory

underpinning' of the position of internet intermediaries. His proposals included ex ante backstop regulation and codes of practice in respect of content in each domain of intermediary activity.

12. Robin Foster's focus was specifically in respect of media pluralism and news in particular. In fact, as we have recently seen, Facebook and Google's dominance across several markets makes them more significant than simply in the area of news. I suggest creating a new category of Information Utilities for specific markets such as search and social media. Information Utilities would be licensed as such and they would have specific reporting regulations in respect of the regulator, which would be granted strong back-stop intervention powers. Dominant Information Utilities – whose dominance might be measured in terms of their significant market power, possibly according to, for example, their share of the online or mobile advertising markets – would have the most stringent reporting duties.

13. There would need to be a lead regulator in respect of this new framework for Information Utilities, which should additionally be charged formally with convening regular meetings with other relevant regulators. Such a framework should be put in place with an expectation that it would be reviewed after a specified period.

14. We know that regulatory interest can 'nudge' dominant players to modify behaviours, as the outgoing former Ofcom chief executive, Ed Richards, told your Lordships' Committee in November 2014. The ability to 'nudge' behaviour away from what society would regard as undesirable is inevitably more effective if transgressing companies are aware that back-stop powers are available to regulators.

11 May 2018

ARTICLE 19 - written evidence (IRN0095)

1. Is there a need to introduce specific regulation for the Internet? Is it desirable or possible?

1. ARTICLE 19: Global Campaign for Free Expression (ARTICLE 19) is an independent human rights organisation that works around the world to protect and promote the rights to freedom of expression and freedom of information. ARTICLE 19 has significant experience working on intermediary liability issues. We intervened in *Delfi v Estonia* before the Grand Chamber of the European Court of Human Rights[12] and have responded to numerous EU consultations on this issue.[13] We have also dealt with intermediary liability and related online content regulation issues in a range of countries, from Brazil[14] or Tanzania[15] to France[16] and Germany[17].

2. In ARTICLE 19’s view, it is unnecessary to introduce new or specific regulation of the Internet in the sense of online content regulation. Though the current legal framework in this area could be further improved to better protect freedom of expression, we believe that rolling back immunity from liability for social media platforms (and introducing further regulation) would only diminish freedom of expression. To the extent that Internet regulation is thought necessary or desirable, however, ARTICLE 19 believes that its focus should be on strengthening data protection law, online political advertising during elections and competition matters rather than restricting content *per se*.

Social media platforms are already subject to a range of laws and regulations

3. At the outset, we note that the ‘Internet’ is far from unregulated. Indeed, a great many laws already govern various *activities* on the Internet, from e-commerce to cybersecurity, cybercrime or data collection and retention. In our experience, many of those who call for ‘internet regulation’ do not take account of this. Instead, what they appear to refer to is the more specific idea of ‘online *content* regulation’. Indeed, most of these calls seem to concern proposals for regulating ‘social media platforms’, particularly in relation to ‘fake news’, ‘extremism’ or hate speech. Our submission focuses on these latter aspects.

[12] ARTICLE 19’s intervention is available from here.

[13] See e.g. ARTICLE 19’s analysis of the EU Code of Conduct on Combatting Illegal Hate Speech, 2016.

[14] See e.g. ARTICLE 19’s country report on Brazil and the Marco Civil DA Internet, 2015 available from here.

[15] See our analysis of the Tanzania Electronic and Postal Communications (Online Content) Regulations 2018

[16] See ARTICLE 19’s intervention before the Conseil d’Etat regarding website blocking of ‘terrorist’ content, available here.

[17] See ARTICLE 19’s analysis of the ‘NetzDG’ law or Law on the enforcement of the law on social networks, 2017.

4. As noted by this Committee in the call for evidence, some degree of online content regulation already exists in the form of the E-Commerce Regulations 2002 (ECRs), which transposed the E-Commerce Directive 2000 ('ECD') into English law.[18] The original purpose of the Directive was to provide a balance between (i) providing a suitable environment for the development of information society services; (ii) tackling illegal content online; whilst (iii) protecting freedom of expression.

5. The Directive does not focus on 'platforms'[19] as such but on various *activities* of information society service providers, including 'mere conduit', 'caching' and 'hosting'. Of greater relevance to social media platforms is Article 14 ECD, which provides conditional immunity to information society providers for hosting illegal content. If social media platforms fail to remove illegal third-party content 'expeditiously', their immunity falls away and they *may* be held liable if the aggrieved party decides to sue them and wins. As such, social media platforms may be held liable for a wide range of content, from privacy laws, to defamation or intellectual property laws.[20] In this regard, it is worth noting that the ECD applies horizontally, i.e. regardless of the type of content at issue, whether civil or criminal. In practice, however, the position is less clear where the content at issue is criminalised, such as incitement to racial or religious hatred. Generally speaking, the author of the content may be prosecuted and convicted. However, it is unclear that companies should be held criminally liable for content that otherwise constitutes 'an offence' if they fail to remove it. There has never been any serious suggestion up until now that this should be the case.

6. In addition, Article 15 ECD prohibits MS from imposing a "*general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity*". Article 15 therefore provides an important safeguard for Internet intermediaries since any monitoring requirement would immediately fix them with knowledge. Moreover, the prohibition under Article 15 constitutes a vital safeguard for the protection of freedom of expression online as it effectively prohibits Member States from requiring intermediaries to adopt filters as a means of preventing access to potentially unlawful content. Such filters are inherently incapable of distinguishing lawful from unlawful information online, so that there is always a risk that they may restrict access to perfectly lawful content.

7. In essence, both Articles 14 and 15 provide the backbone for the protection of freedom of expression online in the EU. As such, any attempt to undermine or reverse these provisions would have a serious chilling effect on freedom of expression. This is especially so as the scheme of the ECD

[18] The text of the ECD is available from here: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN

[19] The European Commission attempted a definition of platforms for the purposes of its Communication on Online Platforms but that definition was criticized by many as being too vague: https://ec.europa.eu/digital-single-market/en/news/full-report-results-public-consultation-regulatory-environment-platforms-online-intermediaries

[20] See e.g. *Tamiz v Google* [2013] EWCA Civ 68

already has serious shortcomings for the protection of freedom of expression.

The ECD has serious shortcomings for the protection of freedom of expression

8. Article 14 ECD effectively forms the basis of what is known as 'notice and takedown procedures' ('NTD'). The interpretation of this provision has given rise to a great deal of regulatory uncertainty, particularly around what constitutes sufficient notice for the purposes of gaining actual knowledge of "illegality". In particular, ARTICLE 19 and many other human rights and digital groups argue that knowledge of *illegality* can only be obtained by a court order, since only a court or independent adjudicatory body can be in a position to determine the legality of content.[21] However, in practice or in law depending on the country at issue, notice may be given by law enforcement agencies or other public authorities or private parties. In the absence of more detail in the Directive or the ECRs, the level of detail required to file a notice is unclear. This is a matter of concern for organisations such as ours as we believe that the balance of incentives in the ECD is such that social media platforms are more likely to remove content on the flimsiest of accusations lest they face liability. This has a chilling effect on freedom of expression.[22] Equally, we are concerned that 'expeditious' removal of content is increasingly interpreted by governments as a matter of as little as one hour in relation to certain types of content (usually 'terrorist' content).[23] Quite apart from the fact that companies should not be put in the position of determining the legality of content, this is plainly an insufficient timeframe in which to make a properly-informed and carefully-considered determination.

But current regulatory alternatives are worse

9. Despite these shortcomings, ARTICLE 19 believes that it is vital to at least maintain the basic principles underpinning Articles 14 and 15 ECD. The regulatory alternatives currently proposed to deal with illegal content online are, in our view, palpably worse for the protection of freedom of expression online.

   - **Current EU self-regulatory or co-regulatory initiatives are unsatisfactory:** Governments regularly put pressure on companies 'to do more' to tackle illegal or undesirable content line. At EU level, the European Commission has led the adoption by social media platforms of a "voluntary" Code of Conduct on Combatting Illegal Hate Speech.[24] The Commission is also looking to put 'hate speech' regulation within the purview of broadcast regulators under the revised Audio-Visual Media

[21] See for instance the Manila Principles on Intermediary Liability, a global civil society initiative, which has been endorsed by over 100 organisations around the world: https://www.manilaprinciples.org//

[22] See also the concerns expressed by the UN Special Rapporteur on Freedom of Expression, Frank La Rue, in his 2011 report on freedom of expression on the Internet, A/HRC/17/27.

[23] See Recommendation of the European Commission on measures to effectively tackle illegal content online, March 2018: http://europa.eu/rapid/press-release_MEMO-18-1170_en.htm

[24] For more details, see ARTICLE 19's legal analysis of the EU Code of Conduct, *op. cit.*

Services Directive (‘AVMS’).[25] More recently, the Commission published its Communication on tackling illegal content online.[26] ARTICLE 19 is deeply concerned about these initiatives. They effectively deputise censorship powers to online platforms, which are tasked with putting in place mechanisms to remove content as fast possible, usually on the basis of their Terms of Service or community standards and without any of the safeguards provided under international human rights law.

When companies remove content on the basis of their Terms of Service, there is no effective remedy in place to challenge those decisions. To begin with, most online platforms do not have a clear complaint mechanism in place (e.g. Facebook or Twitter). Even when they do, the remedy is entirely within the discretion of the company. Some users have attempted to take online platforms to court over the application of their Terms of Service but apart from jurisdictional issues, the applicable legal standard is that of fairness or reasonableness. To that extent, most removal decisions are likely to be justified.[27] Even when content is removed on the basis of national laws, it is highly unclear that users are notified of an order to remove content and what remedies are available to them. More generally, none of the self-regulatory or co-regulatory mechanisms proposed ever suggest putting in place effective remedies to challenge wrongful removal of content.[28]

- **Learning from the French and German regulatory models:** The French and German governments have adopted discreet laws to deal with specific types of content, terrorism and hate speech respectively. In *France*, decree no. 2015-125 lays down rules for the administrative blocking of websites that condone terrorism or distribute child pornography. Under the decree, a special division of the police forces, tasked with combating information technology crimes, can order ISPs to block access to a list of websites without prior judicial authorisation. The division has the power to decide that a website contravenes French criminal laws on terrorism and child pornography, to request that the editors of the website in question remove the allegedly unlawful content, and, where the editors are not identified on the website or refuse to comply with the removal request, to order ISPs to prevent access to the website in question. A magistrate from the privacy public watchdog CNIL is informed of this decision and may recommend its modification or initiate legal proceedings before an administrative tribunal. If internet users access a blocked website, they are redirected to a Ministry of Interior webpage explaining why access has been blocked. The French model raises several concerns for freedom of expression, particularly the

[25] ARTICLE 19’s concerns about proposals for a revised AVMS Directive are detailed here: https://www.article19.org/resources/new-eu-legislation-must-not-throttle-online-flows-of-information-and-ideas/

[26] ARTICLE 19’s concerns with the Communication are detailed here: https://www.article19.org/resources/eu-fails-to-protect-free-speech-online-again/

[27] See for instance the recent French court decision concerning the removal of the painting *L’Origine du monde,* by Courbet: https://www.theartnewspaper.com/news/french-court-makes-mixed-ruling-in-courbet-censorship-case

[28] As an exception, the EU Communication on Tackling Illegal Content makes some weak reference to counter-notices.

use of blocking without judicial approval.[29] At the same time, it is worth noting that some limited safeguards are in place, including the role of the magistrate within the CNIL that can ultimately lead to decisions being challenged in court.

In *Germany*, the Act to Improve Enforcement of The Law on Social Networks (or 'NetzDG') came into force in October 2017.[30] The Act establishes an intermediary liability regime that incentivises, through severe administrative penalties of up to 5 million Euros, the removal and blocking of "clearly violating content" and "violating content", within time periods of 24 hours and 7 days respectively. As regulatory offences, it is possible for the maximum sanction to be multiplied by ten to 50 million Euros. Though the Act does not create new content restrictions, it compels content removals on the basis of select provisions from the German Criminal Code, many of which raise serious freedom of expression concerns in and of themselves, including prohibitions on "defamation of religion". The threshold at which the failures of a Social Network's content removal and blocking processes will be considered systemic enough to attract administrative liability is unclear, and ambiguity in the definitions of key terms (including of "Social Network") is likely to create an environment wherein lawful content is routinely blocked or removed as a precaution. The secondary review that would be provided by "self-regulation institutions", and the limited oversight provided by the Administrative Courts do nothing to address over-blocking, and provide little protection or due process to Social Networks that in good faith refrain from blocking or removing content in the interests of respecting freedom of expression. Just over 6 months after its coming into force, the new German law has already led to over-vigorous removal of content and discussions are underway to amend it.[31]

Redressing the imbalance of power between social media platforms and other actors

10. ARTICLE 19 believes that, to the extent that state intervention might be needed, it should be focused on strengthening data protection law and the legal framework governing online political advertising during elections. Consideration should also be given to any leverage that could be obtained from competition law in order to redress the imbalance of power between platforms and other actors. Obligations related to the portability of data and interoperability of computer systems could potentially contribute to greater competition in this area. Further research should also be conducted into the extent to which the bargaining power of media actors may be strengthened to allow fairer sharing of advertising revenue with social media platforms.

2. What should the legal liability of online platforms be for the content that they host?

[29] For more details about those concerns, please see ARTICLE 19 supports challenge to lawfulness of administrative website blocking, 30 July 2015

[30] ARTICLE 19's detailed legal analysis of the NetzDG law, *op. cit.*.

[31] See Thomson Reuters, Germany looks to revise social media law as Europe watches, 08 March 2018

11. ARTICLE 19 believes that online platforms should remain broadly immune for the third-party content that they host on their platform unless they directly intervene in that content.[32] We also believe that the notice-and-notice model of liability should be further explored, for instance in relation to copyright claims.[33] We further recognise that different types of content may call for slightly different regulatory approaches.[34] More generally, we would like to see stronger procedural safeguards in place to prevent the wrongful removal of content.[35]

12. By contrast, we are concerned about current debates in the UK and the EU that either seek to reverse the conditional immunity principles under the ECD[36] or actively seek to undermine them.[37] Although the current conditional immunity model is not without its problems (see Q1 above), we believe that its core principles should remain in place, i.e. immunity from liability until actual knowledge of illegality is obtained and a prohibition on general monitoring (Article 15 ECD).

13. We also believe that the current focus on liability of social media platforms and analogies with publishers is misguided. Social media platforms engage in three different types of activities: (i) they may produce content of their own, in which case the same liability should apply to them as publishers; (ii) they host content produced by third parties; and (iii) they distribute content, i.e. through the use of algorithms, they make certain types of content more visible and accessible to their users. This is often described as an editorial function or curation of content. However, it does not involve the production of content itself. As such, it should not attract any liability.[38] In this sense, this is not unlike newspapers deciding which stories ought to be published on the frontpage of their broadsheets, those that only get a small mention at the back, and those that are never reported. Newspapers are not held *liable* for these kinds of editorial choices - i.e presentation or selection of content that is placed more prominently for users to read - but for the *content* of their articles. This, however, should not preclude greater transparency and therefore accountability in this area.[39]

14. In relation to third-party content hosted by platforms, the current position as it has developed in the case-law of the Court of Justice of the European Union ('CJEU') is that in order for an Internet service provider to be

[32] See for instance Four Special Rapporteurs on Freedom of Expression, Joint Declaration on Freedom of Expression and the Internet (2011); ARTICLE 19, *Internet Intermediaries: Dilemma of Liability* (2013); the Manila Principles on Intermediary Liability, *op. cit*.

[33] This is already the case in England and Wales with the Defamation Act 2013. See also our policy brief, *Dilemma of Liability, op. cit.*

[34] *Ibid.*

[35] See Manila Principles on Intermediary Liability, *op. cit.*

[36] See Committee on Standards in Public Life, *Intimidation in Public Life: a Review by the Committee on Standards in Public Life,* December 2017, page 36.

[37] See EU Communication on Tackling Illegal Content, *op. cit.*

[38] This is unless the platforms have sufficiently intervened in the content such that it might be understood to be their own: see Graham Smith, *The Electronic Commerce Directive - a phantom demon?* 30 April 2018: https://www.cyberleagle.com/2018/04/the-electronic-commerce-directive.html

[39] Nor would it preclude liability under the ECD if the platforms have sufficiently intervened in the content so as to give it control over it – see Case C-324/09 *L'Oreal and others* [2011] ECR I-06011 *('L'Oreal v eBay')*, para. 123.

considered a host it must be "neutral", i.e. the service provider must not have played an "*active role so as to give it knowledge of, or control over, the data stored*."[40] For instance, when an information society provider such as eBay knowingly provides assistance to sellers by optimizing the presentation of their goods, it loses immunity from liability in relation to this content. [41] At the same time, acting non-neutrally in relation to some user content does not affect hosting protection for other user content, which has not been controlled.[42]

15. In other words, the current model of legal liability *already* takes into account whether or not online platforms are active or passive. The mere fact that social media platforms have terms of service and policies for the removal of content is generally not enough for immunity from liability to fall away and for them to be considered as publishers in the absence of notification.[43] Moreover, it is important to remember that the very architecture of the ECD is designed so as to encourage a degree of self-regulation by platforms whilst protecting them from liability when they try to act as 'Good Samaritans'.[44]

16. Ultimately, ARTICLE 19 argues that at a minimum, the current conditional immunity from liability model should be retained as the least damaging to freedom of expression compared to current proposals. At the same time, we are concerned that under pressure from governments, companies have been encouraged to deploy the use of algorithms to take down content - often in opaque ways and such that content may be prevented from even being published in the first place without any scrutiny.[45] ARTICLE 19 therefore suggests exploring the possibility of establishing new models of self-regulation for social media (e.g. 'social media council'), inspired by the effective self-regulation models created to support and promote journalistic ethics. With some adjustments, the models could be explored for a variety of content regulation issues. For more details, please see our response to Q3.

3. How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

17. ARTICLE 19 notes that companies have become somewhat more transparent about their internal content moderation processes over the years. We now know for example that they use algorithms to identify e.g.

[40] See *Google France, SARL and Google Inc. v. Louis Vuitton Malletier SA and Others,* Cases C-236/08 to C-238/08 *Google France & Google* [2010] ECR I-2417.

[41] See *L'Oreal v eBay*, *op.cit.* at para. 123.

[42] *Ibid*.

[43] See *Tamiz v Google,* [2013] EWCA Civ 68. For a case comment on the decision, see e.g. here.

[44] See Recital 40 ECD "*this Directive should constitute the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information; such mechanisms could be developed on the basis of voluntary agreements between all parties concerned and should be encouraged by Member States; it is in the interest of all parties involved in the provision of information society services to adopt and implement such procedures* (…)". The same reasoning underpins section 230 of the US Communications Decency Act 1996.

[45] This is usually the case of videos, which have been previously flagged as being e.g. 'terrorist' content.

terrorist content or child abuse images. They have also become more upfront about the use of trusted flaggers, whose content takedown notices are fast-tracked for review. Similarly, companies such as Twitter and Facebook have updated and sought to clarify their Terms of Service and online content policies.[46] They have also improved their Transparency Reports so that Twitter, for example, publishes government takedowns requests on the basis of its Terms of Service.[47]

18. However, significant problems remain. Community standards are often coined in broad terms that fall below international standards on freedom of expression. They also ban content that may be lawful under national law. It is unclear how algorithms are used and the extent to which legitimate content is removed.[48] Appeals processes, when they exist, are not easily accessible and short on detail and procedural safeguards. For instance, Facebook recently announced that it would 'expand' its appeals process.[49] However, the announcement so far suggests that individuals are not notified that a request has been made to remove their content and therefore given an opportunity to challenge a content takedown request *prior* to a removal decision. Even if a review process takes place ex post facto for reasons of practicality, it is unclear that users are told the reason for the removal and what the review entails, e.g. whether the decision is taken by the same person. Ultimately, social media platforms retain huge discretion in relation to content removal and whether to grant a remedy.

19. For this reason, we believe that social media platforms should at a minimum comply with the UN Guiding Principles on Business and Human Rights and the standards outlined in the Manila Principles on Intermediary Liability.[50] The Santa Clara Principles on Transparency and Accountability in Content Moderation are also a helpful starting point.[51] See also our response to Q5 and 6 below.

20. At the same time, ARTICLE 19 believes that other solutions are needed to provide greater transparency and accountability for platforms' decisions to remove content and the way in which they distribute content. For this reason, we suggest the creation of independent self-regulatory bodies for social media (e.g. 'social media councils' or 'SMCs'). Our proposal is set out in more detail elsewhere[52] and remains open for discussion but the councils would essentially present the following features:

    - SMCs would deal with content moderation issues (whether one or more), including user complaints about wrongful removal;

[46] For instance, Facebook updated its community standards in April 2018.

[47] https://transparency.twitter.com/en/gov-tos-reports.html

[48] YouTube's latest transparency report seems designed to showcase the amount of content removed on its platform but it begs the question whether all of that content is illegitimate: https://transparencyreport.google.com/youtube-policy/overview

[49] https://newsroom.fb.com/news/2018/04/comprehensive-community-standards/

[50] *Op. cit.*

[51] The Santa Clara Principles are available from here.

[52] See ARTICLE 19, *Self-regulation and hate speech on social media platforms*, March 2018

- SMCs would be funded by social media companies and relevant stakeholders;
- SMCs would be established at national level with some international coordination;
- SMCs would elaborate ethical standards that would be specific to online distribution of content and would cover topics such as the terms and conditions, the community guidelines and the practices of content regulation of social media companies;
- Through light sanctions mainly relying on transparency, peer and public pressure, these mechanisms would promote and ensure respect of appropriate ethical standards by social media companies;
- By making its work transparent to the general public, and through appropriate consultative processes, social media councils could provide a public forum for important public discussions on the regulation of online distribution;
- Their transparency and openness, combined with independence, would give them the credibility they would need to gain public trust.

21. ARTICLE 19 recognises that - as with the development of any new system - the creation of a self-regulatory mechanism for social media is likely to raise a number of difficult questions. As the experience of establishing press councils shows, it can be a lengthy and complex process, as all stakeholders need to agree on a system that they all can make their own. Notwithstanding this, ARTICLE 19 believes that a new system can only come to existence and prove its effectiveness if all participants are willing to make it work. By shifting the focus towards the process rather than trying to impose a solution, a self-regulatory mechanism could allow for the adoption of adapted and adaptable remedies unhindered by the threat of heavy legal sanctions.

22. Developing the new system of independent self-regulation could also provide a solid reference framework to assess the initiatives undertaken by dominant social media companies and their partners so far. It would enable an assessment as to whether they are sufficiently inclusive of all the relevant stakeholders and whether they work in the public interest or are captured by private or special interests; the public would also find out what decisions have been made internally and when they have been subject to external, independent review. Ultimately, the new system would provide greater accountability to the public.

4. What role should users play in establishing and maintaining online community standards for content and behaviour?

23. ARTICLE 19 believes that users and other stakeholders such as civil society organisations can play a useful role in shaping companies’ online content

policies. As such, initiatives such as Facebook's Hard Questions series,[53] which sometimes calls for input from users, are welcome. Equally, we believe that users can play an important role in challenging other users' comments, particularly when they amount to incitement to discrimination, harassment etc. or are merely offensive. The controls provided by companies, for example to block users, may also be useful in mediating interactions between users, e.g. in order to prevent harassment or abuse. At the same time, we would caution against giving users a 'hecklers' veto' over what content should stay up or be removed on online platforms. Users are unlikely to be familiar with the intricacies of e.g. 'hate speech'.[54] If put in charge of policing online content, it is highly likely that vast amounts of minority opinions that people simply do not like or find offensive would be taken offline.

5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

24. ARTICLE 19 believes that the protection of freedom of expression requires companies to be far more transparent and accountable in their online content removal practices. At the minimum, this means that:[55]

- **Community standards should comply with international standards on freedom of expression**. In particular, Internet companies should provide specific examples as to the way in which their standards are applied in practice (e.g. case studies). This should be accompanied by guidance as to the types of factors that are taken into account in deciding whether or not content might be restricted.

- **Companies should conduct regular reviews of their Terms of Service** to ensure compliance with international standards on freedom of expression both in terms of formulation and in practice. In particular, companies should conduct regular audits/human rights impact assessments designed to monitor the extent to which content moderation policies adhere to the principle of non-discrimination. This would at least go some way towards guaranteeing the free expression rights of minority and marginalised groups. Any changes in companies' community standards as a result of such reviews/ human rights impact assessments should be clearly notified to users.

- **Online platforms should not require the use of real names** in order to comply with international standards on privacy. At the very least, Internet companies should ensure anonymity remains a genuine option. Equally, social media platforms should not require their users to identify themselves by means of a government-issued document or other form of identification.

[53] https://newsroom.fb.com/news/category/hard-questions/

[54] See, for instance, ARTICLE 19, *Hate Speech Explained: a Toolkit*, 2015

[55] See also the Manila Principles on Intermediary Liability, *op. cit.*

- **Online platforms should ensure that sanctions for failure to comply with their community standards are proportionate**. In particular, companies' should be clear and transparent about their sanctions policy; and apply sanctions proportionately so that the least restrictive technical means should be adopted. In particular, the termination of an account should be a measure of last resort that should only be applied in the most exceptional and serious circumstances.

- **Online platforms must put in place internal complaints mechanisms:** In particular, individuals should be given notice that a complaint has been made about their content. They should also be given an opportunity to respond *before* the content is taken down. In order for them to respond, the notice of complaint should be sufficiently detailed. If the intermediary concludes that the content should be removed or other restrictive measures should be applied, individuals should be notified of the reasons for the decision and given a right to appeal the decision. In circumstances where the intermediary has put in place an internal mechanism, whereby it takes down content merely upon notice, we believe that at the minimum, the intermediary should: **(i)** require the complainant to fill out a detailed notice, i.e. identifying the content at issue, explaining their grounds for seeking the removal of content; provide contact details of the complainant and a declaration of good faith; **(ii)** notify the content producer that their content has been removed or any other measure that has been applied to their account; **(iii)** give reasons for the decision; and **(iv)** provide and explain internal avenues of appeal.

- **Online platforms should collaborate with other stakeholders to develop new independent self-regulatory mechanisms**, as outlined in Q3.

6. In what ways should online platforms be more transparent about their business practices — for example in their use of algorithms?

25. ARTICLE 19 believes that online platforms should be more transparent about their business practices in a number of areas:

- **Clearer terms of services and more accessible complaints mechanisms:** ARTICLE 19 notes that major social media platforms have amended their community standards a number of times over the years. Unlike amendments to their privacy policy, however, users do not generally get individually notified about changes to community standards. These announcements are generally made in a company press release. In our view, this should change. Companies should notify their users about any changes to their policies. Moreover, companies' terms of service continue to be drafted in broad terms. As noted above, it is vital that companies provide case studies / examples of the way in which they apply their community standards in practice. This would at least help users better understand the rationale behind certain decisions, which may otherwise appear biased or lacking in consistency. Finally, we note that complaints mechanisms for the wrongful removal of content, if any, remain hard to find on companies' websites. In our view, their accessibility should be improved.

- **Use of algorithms**: ARTICLE 19 believes that companies should be far more transparent about the way in which they use algorithms or 'artificial intelligence'.[56] We note, for example, that the Committee of Ministers of the Council of Europe has called on Member States to take "all necessary measures to ensure that Internet intermediaries fulfill their responsibilities to respect human rights in line with the United Nations Guiding Principles on Business and Human Rights". According to the Committee of Ministers, this means, amongst other things, that: [57]

  "Internet intermediaries should clearly and transparently provide meaningful public information about the operation of automated data processing techniques in the course of their activities, including the operation of algorithms that facilitate searches based on user profiling or the distribution of algorithmically selected and personalised content, such as news. This should include information on which data is being processed, how long the data processing will take, which criteria are used, and for what purpose the processing takes place".

  In other words, transparency need not be absolute but should be meaningful to ensure fairness and accountability.

- **Use of trusted flagger scheme:** Social media platforms rely on 'trusted flaggers' to report certain types of content. The assumption is that those flaggers can be trusted to identify e.g. 'hate speech', 'terrorist content' etc. and that they will provide more detailed reports of violations of company community standards or the law. As such, notices by trusted flaggers are more likely to lead to prompt removal. However, very little information is available about how the scheme operates, e.g. who those trusted flaggers are in a given country, what criteria are applied to qualify as trusted flaggers, what proportion of content is removed as result of notices filed by trusted flaggers etc.

- **Transparency reports**: Companies' reporting of content removals has improved over the years. For instance, Twitter now reports content removed on the basis of its Terms of Service when the removal has been requested by the authorities.[58] However, companies continue to shy away from providing data about content removed on the basis of their own terms of service at their own initiative (e.g. through filtering) or upon request from third parties. Companies sometimes oppose the need to protect users' privacy as a reason for not providing this information. However, we believe that this should not apply in the case of lawyers or trusted flaggers, which often include copyright holders associations or other interest groups. Finally, companies should provide information about the number of complaints they receive about alleged wrongful

[56] See ARTICLE19's written evidence to the House of Lords Select Committee on Artificial Intelligence, September 2017

[57] See Recommendation CM/Rec (2018)2 on the roles and responsibilities of internet intermediaries.

[58] https://transparency.twitter.com/en/gov-tos-reports.html

removals of content and the outcome of such complaints (i.e. whether content was restored or not).

7. What is the impact of the dominance of a small number of online platforms in certain online markets?

26. **ARTICLE 19 notes that, at present, there is much more information available online than ever before and that social media platforms have greatly contributed to this state of affairs. However, the dominance of a small number of online platforms remains a matter of concern. In particular, the behaviour of dominant social media platforms has the potential in some instances to become a barrier to entry in the marketplace of ideas. In our view, this might in certain circumstances warrant state intervention under Article 10 of the European Convention on Human Rights, as States' positive obligation to ensure pluralism and diversity of the media" (see also Q1).**

8. What effect will the United Kingdom leaving the European Union have on the regulation of the Internet?

27. ARTICLE 19 notes that Article 15 ECD (general monitoring) was not expressly transposed in the E-Commerce Regulations 2002. This raises the prospect that the UK may wish to impose general monitoring obligations in future legislation, particularly as the UK has signaled that it did not wish to fully align with EU legislation in this area.[59] If that were to be the case, we believe that this would constitute a serious interference with the rights to freedom of expression and privacy. This would be out-of-step with major international standards on freedom of expression and privacy in this area.[60] More fundamentally, proactive filtering would mean all expression mediated by algorithms, which are inherently incapable of detecting nuance or context, i.e. the very elements that might make the difference between lawful and unlawful speech. As Graham Smith, partner at Bird & Bird as noted, "*Article 19 of the 1948 Universal Convention on Human Rights is not predicated on the assumption of mediated speech*."[61] General monitoring would effectively delegate censorship powers to private companies and amount to a form of prior restraint. As such, we strongly urge the Committee to refrain from any recommendation that would undermine the prohibition of general monitoring on the Internet.

May 2018

[59] For the implications of such divergence, see e.g. Graham Smith, *The Electronic Commerce Directive - a phantom demon? Op. cit.*

[60] See e.g. UN Special Rapporteur on freedom of expression, A/HRC/17/27 (2011); Four Special Rapporteurs on Freedom of Expression, *Joint Declaration on Freedom of Expression and the Internet* (2011) and more recently, the *Joint Declaration on Freedom of Expression and Fake News, Disinformation and Propaganda* (2017)

[61] See Graham Smith, *Time to speak up for Article 15,* 21 May 2017: https://www.cyberleagle.com/2017/05/time-to-speak-up-for-article-15.html

Association for Proper Internet Governance – written evidence (IRN0001)

1. This submission provides evidence in response to the call at: https://www.parliament.uk/business/committees/committees-a-z/lords-select/communications-committee/news-parliament-2017/internet-regulation-inquiry-launch/

A. Summary

2. This section presents the summary of our replies to the following questions:

1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

   Yes, there is a need for specific regulation, in particular at the international level, for various aspects of the Internet. See the substantive comments in sections B and C below.

2. What should the legal liability of online platforms be for the content that they host?

   There should be harmonized international norms regarding this matter, see section C.3 below.

3. How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

   There should be harmonized international norms regarding this matter, see sections C.2 and C.3 below.

4. What role should users play in establishing and maintaining online community standards for content and behaviour?

   There should be harmonized international norms regarding this matter, see sections C.2 and C.3 below.

5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

   There should be harmonized international norms regarding this matter, see sections C.2 and C.3 below.
6. What information should online platforms provide to users about the use of their personal data?

There should be harmonized international norms regarding this matter, see section C.1 below.

7. In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

   There should be harmonized international norms regarding this matter, see sections C.1, C.9 and C.10 below.

8. What is the impact of the dominance of a small number of online platforms in certain online markets?

   There is a large impact. There should be harmonized international norms to address this issue, see sections C.9 and C.10 below.

9. What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

   Hopefully it will reduce the tendency of the European Union to refuse to regulate and to follow US neo-liberal policies regarding the Internet.

B. Importance of International Policies

3. The document E/CN.16/2015/CRP.2[62], "Mapping of international Internet public policy issues", 17 April 2015, of the UNCTAD Working Group on Enhance Cooperation (WGEC) states in Chapter 9, Concluding remarks:

> The tension between the transborder nature of the Internet, on the one hand, and predominantly national regulations that govern public policy issues pertaining to the Internet, on the other, results into challenges for the implementation of regulation. Making diverse legislation more interoperable and aligning national laws with existing international instruments helps in overcoming these challenges. At the international level, this calls for strengthened cooperation, capacity building and sharing of information and best practices.
> The review indicates that improvements could be made in respect of these gaps. At international level, strengthened coordination and collaboration across stakeholder groups will be critical in efforts to bridge them.

4. We concur with that finding and are of the view that the rule of law must exist at the international level for the Internet, given that the Internet is an international phenomenon. Further, the Internet is affecting all walks of life and this creates challenges for governments.[63] As the Internet Society puts the matter in its *2017 Global Internet Report: Paths to our Future*[64]: "As the Internet

[62] http://unctad.org/meetings/en/SessionalDocuments/ecn162015crp2_en.pdf

[63] See for example pp. 3 ff. of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*, available at: http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872

[64] https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf

grows and expands into more areas of our economy and society, **Governments** will be faced with a host of new and complex issues that will challenge all aspects of their decision-making." The same report states on page 70: "With increasing international data flows, services and goods will come a need to agree on international norms. Some predict that, in the absence of an agreement on universal norms, regional agreements will multiply and accelerate the emergence of a multipolar world organised around new blocs of countries and societies."

5. UNCTAD makes similar points in its Information Economy Report 2017: Digitalization, Trade and Development[65]:[66]

> Digitalization will create opportunities for entrepreneurs and businesses, while also bringing enormous benefits to consumers. However, at the same time it will disrupt existing practices, expose incumbents to competition, change skills requirements of workers and result in job losses in some countries and sectors.
>
> …
>
> Like previous large-scale economic transitions, the benefits will be immense, but they will not materialize through a smooth, cost-free process. The net outcome will depend on policies undertaken at both national and international levels to build countries' capabilities to take advantage of these transformations.

6. Similar points are made in the Report of the 6-8 December 2016, Mexico City, UN Expert Group Meeting on Exponential Technological Change, Automation, and Their Policy Implications for Sustainable Development[67] ("exponential technologies" refers to technologies that exhibit exponential growth, including big data, artificial intelligence, the Internet, etc.). And in one expert's predictions for 2018[68] and in a recent book from a major ICT company[69] and an article by a well-known Internet engineer[70].

7. These are not new thoughts. As a scholar put the matter back in 2002[71]:

> "In the early years of Internet development, the prevailing view was that government should stay out of Internet governance; market forces and self-regulation would suffice to create order and enforce standards of behavior. But this view has proven inadequate as the Internet has become mainstream. A reliance on markets and self-policing has failed to

[65] http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872

[66] The citation is from p. iv.

[67] https://sustainabledevelopment.un.org/content/documents/15295Meeting_report_final.pdf . Additional papers on achieving the Sustainable Development Goals are published at: https://sustainabledevelopment.un.org/index.php?menu=1027

[68] https://www.diplomacy.edu/blog/2018predictions

[69] https://blogs.microsoft.com/blog/2018/01/17/future-computed-artificial-intelligence-role-society/

[70] Andrew Sullivan, "Avoiding lamentation: to build a future Internet", *Journal of Cyberpolicy*, vol. 2, no. 3, pp. 323-337, available at: http://www.tandfonline.com/doi/full/10.1080/23738871.2017.1400083

[71] Baird, Zoe (2002) "Governing the Internet: Engaging Government, Business, and Nonprofits", *Foreign Affairs*, vol. 81, no. 6, November/December 2002. Available at: http://www.markle.org/sites/default/files/06_baird_15_20_0.pdf

> address adequately the important interests of Internet users such as privacy protection, security, and access to diverse content. And as the number of users has grown worldwide, so have calls for protection of these important public and consumer interests. It is time we accept this emerging reality and recognize the need for a significant role for government on key Internet policy issues."

8. There is general agreement that Brexit and the election of US President Trump were driven by dissatisfaction with the results of globalization, that is, unequal distribution of the benefits[72]. Even the July G20 Leaders' Declaration acknowledges that "globalization has created challenges and its benefits have not been shared widely enough"[73]. Or, in other words, we strove to increase efficiency but forgot to maintain equity[74]. As The Economist Intelligence Unit puts the matter[75]:

> The parallels between the June 2016 Brexit vote and the outcome of the November 8th US election are manifold. In both cases, the electorate defied the political establishment. Both votes represented a rebellion from below against out-of-touch elites. Both were the culmination of a long-term trend of declining popular trust in government institutions, political parties and politicians. They showed that society's marginalised and forgotten voters, often working-class and blue-collar, do not share the same values as the dominant political elite and are demanding a voice of their own—and if the mainstream parties will not provide it, they will look elsewhere.

9. As the Secretary-General of UNCTAD put the matter when introducing UNCTAD' Trade and Development Report 2017: "the world economy remains unbalanced in ways that are not only exclusionary, but also destabilizing and dangerous for the political, social and environmental health of the planet. Even when economic growth has been possible, whether through a domestic consumption binge, a housing boom or exports, the gains have disproportionately accrued to the privileged few."[76]

[72] See for example the last paragraph at: http://fortune.com/2017/02/18/bill-gates-robot-taxes-automation/

[73] Page 2 of https://www.g20.org/gipfeldokumente/G20-leaders-declaration.pdf . The same point is made on p. 3: "We recognise that the benefits of international trade and investment have not been shared widely enough. We need to better enable our people to seize the opportunities and benefits of economic globalisation." See also
page 11 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872

[74] http://www.other-news.info/2017/02/our-collective-failure-to-reverse-inequality-is-at-the-heart-of-a-global-malaise-2/ and
http://www.other-news.info/2017/06/myths-of-globalization-noam-chomsky-and-ha-joon-chang-in-conversation/ and paragraph 4.6.2 of
http://congress.world-psi.org/wp-content/uploads/2017/05/EN-PoA-final-May-2017.pdf ; and
http://wir2018.wid.world/files/download/wir2018-summary-english.pdf ;
for an economic explanation in terms of ICTs, see:
https://www.technologyreview.com/s/608095/it-pays-to-be-smart/

[75] *Democracy Index 2016*, The Economist Business Intelligence Unit, page 14, at:
http://pages.eiu.com/rs/783-XMC-194/images/Democracy_Index_2016.pdf

[76] http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1852

10. As a speaker put the matter at a meeting[77] of a working group of the UN Human Rights Council, referring to the work of the well-known economist Joseph Stiglitz: "… globalization distinctly disadvantaged developing countries … Market failure and the dominant role of finance not only affected inequality between nations, but also within nations, including within advanced economies. … there is a growing trend to combat this."[78]

11. There are two solutions: stop globalizing, which is what Brexit and President Trump are about, or come up with globalized norms that ensure equity. As the Internet Society puts the matter in its report cited above: "Populist trends around the world will undermine decades of interconnected policy goals in ways that could fragment the core architecture of the Internet and undermine its global promise."

12. As WGEC member Parminder Jeet Singh put the matter in an E-Mail:

> The Internet is the public sphere today. It cements how the public organises and expresses. But it quite a bit more: It is a kind of a new nervous system running through the society.
>
> The Just Net Coalition, and its Delhi Declaration[79], believes, that the Internet has to be claimed as a commons and as a public good. Not a market or competitive good. It is the level playing field of the society, on which opportunities can be sought, and made good -- in a manner that is equitable for all.
>
> Internet's basic structures and layers -- whether the physical telecom layer; its key social applications, like search, social media, instant media, etc; or big data and digital intelligence, must be treated as commons, society's common property, and governed accordingly. This has to be the point of departure for Internet governance, not merely as a commonly used rhetoric, but as an actual first political principle. Things will change from then on!
>
> The original sin was when the US cast the Internet in a primarily commercial mode - with its first Internet related policy framework of "A framework for global e-commerce". One can be sure that an Internet born and nurtured in, say, a nordic country, or a developing one, would have had a different default nature. And because, with the Internet, the very playing field of the society was able to be rigged by big business, the period of coming of age of the Internet in the first decade and half of this millennium has also been of one of the fastest ever growth of inequality in the world. we must investigate this connection, and remedy it, for us to win the war against unsustainable inequality. It is vain, in these circumstances, to keep giving air to the myth of Internet's egalitarianism, it is evidently not so. Not as we have come to know it.

[77] http://ohchr.org/EN/HRBodies/HRC/WGTransCorp/Session3/Pages/Session3.aspx

[78] See paragraph 35 of the report at: http://ohchr.org/Documents/HRBodies/HRCouncil/WGTransCorp/Session3/DraftReportThirdSession.docx

[79] http://www.justnetcoalition.org/delhi-declaration

> Can it be made egalitarian. Yes, for which see above :). We must reclaim the (equal) playing field nature of the Internet.

13. As the UK Conservative Party put the matter in its Manifesto of 2017[80]:

> The internet is a global network and it is only by concerted global action that we can make true progress.
>
> We believe that the United Kingdom can lead the world in providing answers. So we will open discussions with the leading tech companies and other like-minded democracies about the global rules of the digital economy, to develop an international legal framework that we have for so long benefited from in other areas like banking and trade. We recognise the complexity of this task and that this will be the beginning of a process, but it is a task which we believe is necessary and which we intend to lead.
>
> By doing these things – a digital charter, a framework for data ethics, and a new international agreement – we will put our great country at the head of this new revolution; we will choose how technology forms our future; and we will demonstrate, even in the face of unprecedented change, the good that government can do.

14. The time has come to face this issue square on for what concerns Internet governance. Should we do nothing, and watch as the Internet becomes less global, or should we work towards international norms that will allow the Internet to remain global? As a senior official of the European Commission put the matter regarding the future of the Internet[81]: "We must address the real concerns of citizens, such as lack of trust, choice and respect and worst of all lock-in effects."

15. And global issues are Internet issues, make no mistake about it. According to Oxfam[82], eight men owned, in 2017, as much wealth as the poorest 50% of the world's population. Of those eight[83] men, five are in ICT industries: Gates, Slim, Bezos, Zuckerberg and Ellison.

16. There is a lack of competition at the international level. As a scholar puts the matter: "when we look at what the digital economy has done over the past two decades, what becomes clear is that it has created an enormous amount of value for consumers and for a small group of big companies, even as it has diminished competition, centralised power, and made life much more difficult for businesses that produce content or try to compete with the economy's dominant players."[84] The advent of the Internet has favored concentration and this has contributed to rising income inequality.[85]

[80] See p. 83 of: https://s3.eu-west-2.amazonaws.com/manifesto2017/Manifesto2017.pdf

[81] https://ec.europa.eu/digital-single-market/en/blog/what-future-internet

[82] https://www.oxfam.org/en/pressroom/pressreleases/2017-01-16/just-8-men-own-same-wealth-half-world

[83] http://www.forbes.com/billionaires/list/#version:static

[84] https://www.technologyreview.com/s/607954/why-tesla-is-worth-more-than-gm/ ; see also the first paragraph of Wu, Tim, Antitrust Via Rulemaking: Competition Catalysts (October 24, 2017), *Colorado*

17. Apparently the OECD recognized the importance of international digital policy (which includes international Internet policy) when it created its Committee on Digital Economic Policy in 2014 to, inter alia, "Develop and promote a coherent policy and regulatory framework which supports competition, investment and innovation across the digital economy".[86] Further, the OECD launched a "Going Digital" horizontal project at the start of 2017; a paper intended to provide Ministers with a first and preliminary set of policy conclusions that are emerging from OECD work on the digital transformation was presented to the 7-8 June Meeting of the OECD Council at the Ministerial Level; that paper is titled "Going Digital: Making the Transformation Work for Growth and Well-Being"; it covers many of the issues referred to below.[87]

18. If these issues are worthy of consideration within the OECD, then surely they are also worthy of consideration at the global level, in particular because many of the issues significantly affect developing countries. We note the UNCTAD has initiated some discussions, albeit in the form of an Intergovernmental Group of Experts and for the narrow topic of E-Commerce.[88] Several of the issues discussed below are mentioned in section II.B, Challenges, of the Note by the Secretariat titled "Maximizing the development gains from e-commerce and the digital economy" (TD/B/EDE/1/2) submitted to the first meeting of the cited Group of Experts.[89] Several of the issues mentioned below are also well summarized in Chapter 4 of ITU, Measuring the Information Society Report 2017, Vol. 1[90].

19. Thus we urge serious consideration of the specific steps towards the second solution mentioned above – how to maintain and grow a global Internet – that are we are recommending. It is in this light that we propose specific recommendations on how to further implement enhanced cooperation as envisioned in the Tunis Agenda.

C. Specific Recommendations

Specific proposed recommendations are shown as text in boxes below.

20. We note that many sections of the cited "Mapping of international Internet public policy issues" identify areas where further study would be appropriate, in particular:

2.7 Net neutrality
2.8 Cloud
2.10 Internet of Things (IoT)

Technology Law Journal, https://ssrn.com/abstract=3058114

[85] https://www.nytimes.com/2016/07/13/business/economy/antitrust-competition-inequality.html

[86] See http://webnet.oecd.org/OECDGROUPS/Bodies/ShowBodyView.aspx?BodyID=1837&Book=True

[87] https://www.oecd.org/mcm/documents/C-MIN-2017-4%20EN.pdf ; see also p. 82 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872

[88] http://unctad.org/en/Pages/MeetingDetails.aspx?meetingid=1437

[89] The Note is available at: http://unctad.org/meetings/en/SessionalDocuments/tdb_ede1d2_en.pdf

[90] https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf

3.1 Cybersecurity
3.2 Cybercrime
3.4 Cyber conflict
3.6 Encryption
3.7 Spam
4.1 Freedom of expression
4.2 Privacy and data protection
5.3 Copyright
5.5 Labour law
5.6 Intermediaries

Recommendation 0.1

We concur with the findings of the document E/CN.16/2015/CRP.2, Mapping of international Internet public policy issues, 17 April 2015, and propose to recommend that all the recommendations for further study in the cited document be endorsed.

21. Discussions that are planned to take place in the context of the World Trade Organization (WTO) could have significant implications for Internet governance[91]. As two experts put the matter[92]:

> One must wonder whether this [negotiations in WTO] will be an opportunity to foster digital rights or leave us with even lower standards and a concentrated, quasi-monopolistic market benefiting from public infrastructure? The rhetoric of opportunities for the excluded – connecting the next billion – sounds great, but only if we disconnect it from the current realities of the global economy, where trade deals push for deregulation, for lower standards of protection for the data and privacy of citizens, where aggressive copyright enforcement risks the security of devices, and when distributing the benefits, where big monopolies, tech giants (so called GAFA) based mostly in the US, to put it bluntly, take them all.
>
> …
>
> Never before has a trade negotiation had such a limited number of beneficiaries. Make no mistake, what will be discussed there, with the South arriving unprepared, will affect each and every space, from government to health, from development to innovation going well beyond just trade. Data is the new oil – and we need to start organising ourselves for the fourth industrial revolution. The data lords, those who

[91] See for example WTO documents JOB/SERV/248/Rev.2 and TN/S/W/64. See in this context our submission to the ITU Council Working Group on Internet-related Public Policy Issues, at: http://www.itu.int/en/council/cwg-internet/Pages/display-June2017.aspx?ListItemID=5 . For an overall analysis of the WTO proposals, see: http://www.huffingtonpost.com/entry/state-of-play-in-the-wto-toward-the-11th-ministerial_us_5951365ae4b0f078efd98399 ; see also: http://www.itu.int/en/council/cwg-internet/Pages/display-June2017.aspx?ListItemID=7 and https://www.diplomacy.edu/blog/2018predictions#3

[92] https://www.opendemocracy.net/digitaliberties/renata-avila-burcu-kilic/new-digital-trade-agenda-are-we-giving-away-internet

> have the computational power to develop superior products and services from machine learning and artificial intelligence, want to make sure that no domestic regulation, no competition laws, privacy or consumer protection would interfere with their plans.
>
> …
>
> Disguised as support for access and affordability, they [dominant Internet data-driven companies] want everyone to connect as fast as they can. Pretending to offer opportunities to grow, they want to deploy and concentrate their platforms, systems and content everywhere in the world. Enforcement measures will be coded in technology, borders for data extraction will be blurred, the ability to regulate and protect the data of citizens will be disputed by supranational courts, as local industries cannot compete and local jobs soar. If we are not vigilant, we will rapidly consolidate this digital colonisation, a neo-feudal regime where all the rules are dictated by the technology giants, to be obeyed by the rest of us.

22. Criticism of holding discussions related to the Internet in the WTO and other trade negotiation forums is not all that recent. Pages 74-75 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*[93] contain the following citations:

> "Bilateral and multilateral free trade agreements can significantly affect Internet governance issues. Many, such as the Trans-Pacific Partnership Agreement, specifically address important issues such as data localization, encryption, censorship and transparency, all of which are generally regarded as forming part of the Internet governance landscape. However, they are negotiated exclusively by governments and usually in secret. At the same time, such agreements substantially benefit the Internet in a myriad of ways, such as by agreeing on rules to improve competition and market access. Further agreements such as the US-Europe Transatlantic Trade and Investment Partnership and the Trade in Services Agreement under the World Trade Organization are expected to cover similar territory. The fact that these negotiations are open only to governments has inspired protests by non-governmental actors demanding that they be informed and engaged in negotiations to allay fears that the new rules embedded in these agreements favour the interests of governments or corporations over those of other Internet users. The closed nature of the negotiations also means that the benefits governments hope to achieve may not be evident to the general public (GCIG, 2016: 78)."[94]

and

> "We recognize the considerable social and economic benefits that could flow from an international trading system that is fair, sustainable,

[93] http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872

[94] The source is the report of the Global Commission on Internet Governance, at: http://ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf .

> democratic, and accountable. These goals can only be achieved through processes that ensure effective public participation. Modern trade agreements are negotiated in closed, opaque and unaccountable fora that lack democratic safeguards and are vulnerable to undue influence. These are not simply issues of principle; the secrecy prevents negotiators from having access to all points of view and excludes many stakeholders with demonstrable expertise that would be valuable to the negotiators. This is particularly notable in relation to issues that have impacts on the online and digital environment, which have been increasingly subsumed into trade agreements over the past two decades."[95]

23. The cited UNCTAD report goes on to state:

> "Stakeholders have also expressed concerns about various substantive aspects of rules governing trade in the digital economy. Contentious issues include the inclusion of provisions concerning intellectual property, encryption, source codes, intermediary liability, network neutrality, spam, authentication and consumer protection."[96]

24. As one academic analysis puts the matter: "The new e-commerce regime is not about 'free trade' and barely about real commerce. As with the WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), it aims to protect and entrench the oligopoly of first movers".[97] The dangers of viewing data as a commodity that should flow freely are well explained in a paper by IT for Change.[98] As two experts put the matter[99]:

> But if all the world's data flows back to a few tech powerhouses, without restrictions or taxes, this will further reinforce their monopolies, widen the privacy gap, and leave developing countries as passive consumers or data points, rather than participants in the digital economy.
>
> Those calling for liberalization use the rhetoric of creating opportunities for the poor — connecting the next billion — which sounds great, but only if we disconnect it from reality. Today, 60% world lacks even access to electricity. In the past, Spanish colonizers arrived in the Americas offering mirrors to the indigenous people in exchange for their gold. Is connectivity the "mirror" powerful actors are offering to the global poor today?

[95] The source is the Open Digital Trade Network Brussels Declaration, at: https://www.eff.org/files/2016/03/15/brussels_declaration.pdf

[96] The cited UNCTAD report gives the following source for that statement: "Bureau Européen des Unions de Consommateurs (BEUC), Analysis of the TiSA e-commerce annex & recommendations to the negotiators, TiSA leaks, September 2016 (http://www.beuc.eu/publications/beuc-x-2016-083_lau_beucs_analysis_e-commerce_tisa_2016.pdf , accessed 1 June 2017); and EDRi's red lines on TTIP, January 2015 (https://edri.org/files/TTIP_redlines_20150112.pdf , accessed 1 June 2017). BEUC and EDRi are coalitions of 43 and 35 civil society organizations, respectively."

[97] Page 2 of Kelsey, Jane (2017) *The Risks for ASEAN of New Mega-Agreements that Promote the Wrong Model of e-Commerce*, ERIA Discussion Paper 2017-10, available at: http://www.eria.org/publications/discussion_papers/DP2017-10.html

[98] http://www.itforchange.net/sites/default/files/add/The%20grand%20myth%20of%20cross-border%20data%20flows%20in%20trade%20deals-Dec2017.pdf

[99] https://www.buzzfeed.com/burcukilic/big-tech-is-pushing-for-a-new-kind-of-free-trade

> Trade agreements eliminate the diversity of domestic policies and priorities, and impose costly restrictions on countries that want to address local inequalities and boost local industry. In the case of the digital economy, it will consolidate the position of few, to the detriment of the rest.

25. The scope of the provisions proposed in free trade negotiations is very broad and goes well beyond what the traditional scope of WTO.[100] And, as the cited scholar[101] puts the matter, citing other scholars: "We find ourselves in '. . . a system that officially claims to embrace free trade, yet still pits one political interest against another in a quest to seize protectionist rents. Powerful lobbies, such as domestic producers, capture trade negotiators and replace national interests with those of their own.'" Negotiations in trade venues proceed "in a secretive, non-transparent, and non-inclusive manner."[102]

Recommendation 0.2

In light of the fundamental importance of transparency and inclusiveness in discussions of international Internet policy matters, we recommend inviting governments to refrain from discussing those matters in forums that are not transparent or inclusive. In particular we recommend inviting governments not to discuss in the context of the WTO or plurilateral forums such as the Trade in Services Agreements (TISA) matters such as the free flow of data or the terms of access to foreign telecommunications infrastructure. We recommend to invite governments to discuss all matters related to Internet governance, including matters such as the free flow of date or the terms of access to foreign telecommunications infrastructure, only in forums that are transparent and inclusive, and in accordance with the roles and responsibilities outlined in paragraph 35 of the Tunis Agenda.

Recommendation 0.3

In light of the fundamental importance of transparency, we recommend inviting all entities involved in Internet governance discussions, including civil society entities, to be transparent with respect to their funding sources.

Recommendation 0.4

In light of the fundamental importance of transparency[103], and of the need to have access to data in order to make evidence-based decisions, we recommend inviting all stakeholders to consider whether it would be appropriate to include a general provision on price transparency in a future international instrument, for example in a future version of the International Telecommunication Regulations (ITRs).

[100] See for example pp. 101 ff. of the academic analysis at: https://lawreview.law.ucdavis.edu/issues/51/1/Symposium/51-1_Burri.pdf

[101] *Op. cit.*, p. 129

[102] *Op. cit.*, p. 130

[103] For a general discussion of the importance of transparency, see : http://www.circleid.com/posts/20171121_transparency_the_internets_only_currency/

26. Further, we have identified some additional areas where further studies would be appropriate. Consequently, we submit specific proposals regarding the following international Internet public policy issues that require more study than is taking place at present:

1. The economic and social value of data and its processing
2. Takedown, filtering and blocking
3. Intermediary liability
4. Privacy, encryption and prevention of inappropriate mass surveillance
5. How to deal with the Internet of Things (IoT)
6. Externalities arising from lack of security and how to internalize such externalities
7. Ethical issues of networked automation, including driverless cars
8. How to deal with the job destruction and wealth concentration induced by ICTs in general and the Internet in particular
9. How to deal with platform dominance
10. How to deal with the increasing importance of embedded software
11. Issues related to ccTLDs and gTLDs
12. Roles and responsibilities

1. The economic and social value of data and its processing

27. It is obvious that personal data has great value when it is collected on a mass scale and cross-referenced.[104] An excellent discussion of this topic, with numerous references, is give in pp. 9 ff. of Third World Network, Briefing no. 3 for the World Trade Organization 11th Ministerial Conference, Buenos Aires, 10-13 December 2017, at: http://www.twn.my/MC11/briefings/BP3.pdf.

28. Indeed, the monetization of personal data drives today's Internet services and the provision of so-called free services such as search engines.[105] These developments have significant implications, in particular for developing

[104] See for example pp. vii and 2 of the GCIG report, available at: http://ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf . Henceforth referenced as "GCIG". See also 7.4 of http://www.oecd-ilibrary.org/taxation/addressing-the-tax-challenges-of-the-digital-economy_9789264218789-en ; and http://www.other-news.info/2016/12/they-have-right-now-another-you/ ; and the study of data brokers at: https://www.opensocietyfoundations.org/sites/default/files/data-brokers-in-an-open-society-20161121.pdf; https://www.internetsociety.org/blog/public-policy/2017/03/my-data-your-business ; http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource; and http://www.itu.int/en/council/cwg-internet/Pages/display-June2017.aspx?ListItemID=7; and https://www.theguardian.com/world/2017/aug/23/silicon-valley-big-data-extraction-amazon-whole-foods-facebook and
pages 6-7 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872 and http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf and https://www.diplomacy.edu/blog/2018predictions#1

[105] http://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041/ and 7.4 of the cited OECD report; and http://www.other-news.info/2016/12/they-have-right-now-another-you/ and https://www.internetsociety.org/blog/public-policy/2017/03/my-data-your-business

countries.[106] Users should have greater control over the ways in which their data are used.[107] In particular, they should be able to decide whether, and if so how, their personal data are used (or not used) to set the prices of goods offered online.[108] It should not be permissible (as it may be at present) for companies to collect data even before users consent to the collection by clicking on a button in a form[109]. The Internet Society recommends the following[110]: "All users should be able to control how their data is accessed, collected, used, shared and stored. They should also be able to move their data between services seamlessly."

29. As the Supreme Court of India put the matter in a recent judgment finding that privacy is a fundamental right: "To put it mildly, privacy concerns are seriously an issue in the age of information."[111]

30. The following joke[112] well illustrates what is happening:

CALLER: Is this Gordon's Pizza?
GOOGLE: No sir, it's Google Pizza.
CALLER: I must have dialed a wrong number. Sorry.
GOOGLE: No sir, Google bought Gordon's Pizza last month.
CALLER: OK. I would like to order a pizza.
GOOGLE: Do you want your usual, sir?
CALLER: My usual? You know me?
GOOGLE: According to our caller ID data sheet, the last 12 times you called you ordered an extra-large pizza with three cheeses, sausage, pepperoni, mushrooms and meatballs on a thick crust.

[106] http://twn.my/title2/resurgence/2017/319-320/cover03.htm; see also page 12 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872

[107] See for example pp. 42, 106 and 113 of GCIG. See also http://www.internetsociety.org/policybriefs/privacy; and http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html; and http://ec.europa.eu/commission/2014-2019/oettinger/announcements/speech-conference-building-european-data-economy_en and http://webfoundation.org/2017/03/web-turns-28-letter/ and https://ec.europa.eu/futurium/en/system/files/ged/ec_ngi_final_report_1.pdf and https://www.internetsociety.org/blog/public-policy/2017/03/my-data-your-business and https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2017/17-03-14_Opinion_Digital_Content_EN.pdf and http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-592.279+01+DOC+PDF+V0//EN&language=EN and https://www.reuters.com/article/us-facebook-spain-fine/facebook-fined-1-2-million-euros-by-spanish-data-watchdog-idUSKCN1BM1OU and https://www.economist.com/news/leaders/21735021-dominance-google-facebook-and-amazon-bad-consumers-and-competition-how-tame

[108] https://www.theguardian.com/technology/2017/jun/04/surge-pricing-comes-to-the-supermarket-dynamic-personal-data

[109] https://gizmodo.com/before-you-hit-submit-this-company-has-already-logge-1795906081?null

[110] Page 107 of the 2017 Global Internet Report: Paths to Our Digital Future, available at: https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf

[111] Paragraph 171 on p. 248. Why this is the case is explained in detail in paragraphs 170 ff. on pp. 246 ff. of the judgment. The full text of the extensively researched 547-page judgment is at: http://supremecourtofindia.nic.in/pdf/LU/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf ; see also the good discussion in paragraphs 21-35, 88-97, and 103-112 of the 19 October 2017 Report of the Special Rapporteur on Privacy, document A/72/43103, http://www.ohchr.org/Documents/Issues/Privacy/A-72-43103_EN.docx

[112] http://www.jokesoftheday.net/joke-Google-s-pizza/2017051897

CALLER: OK! That's what I want …
GOOGLE: May I suggest that this time you order a pizza with ricotta, arugula, sun-dried tomatoes and olives on a whole wheat gluten free thin crust?
CALLER: What? I detest vegetables.
GOOGLE: Your cholesterol is not good, sir.
CALLER: How the hell do you know?
GOOGLE: Well, we cross-referenced your home phone number with your medical records. We have the result of your blood tests for the last 7 years.
CALLER: Okay, but I do not want your rotten vegetable pizza! I already take medication for my cholesterol.
GOOGLE: Excuse me sir, but you have not taken your medication regularly.
According to our database, you only purchased a box of 30 cholesterol tablets once, at Drug RX Network, 4 months ago.
CALLER: I bought more from another drugstore.
GOOGLE: That doesn't show on your credit card statement.
CALLER: I paid in cash.
GOOGLE: But you did not withdraw enough cash according to your bank statement.
CALLER: I have other sources of cash.
GOOGLE: That doesn't show on your last tax return unless you bought them using an undeclared income source, which is against the law.
CALLER: WHAT THE HELL?
GOOGLE: I'm sorry, sir, we use such information only with the sole intention of helping you.
CALLER: Enough already! I'm sick to death of Google, Facebook, Twitter, WhatsApp and all the others. I'm going to an island without internet, cable TV, where there is no cell phone service and no one to watch me or spy on me
GOOGLE: I understand sir, but you need to renew your passport first. It expired 6 weeks ago…

31. Current trends regarding usage of personal data suggest that it "can be used to automatically and accurately predict a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender"[113] and that, on the basis of such data, people might be assigned a score that determines not just what advertisements they might see, but also whether they get a mortgage for their home[114]. In fact, big data is already being used in ways that could lead to social control, see: https://www.wired.com/story/age-of-social-credit/

32. The European Parliament appears to be concerned about such issues, according to a draft report on the proposal for a regulation of the European

[113] http://www.pnas.org/content/110/15/5802.full#aff-1

[114] https://www.theguardian.com/commentisfree/2017/jun/18/google-not-gchq--truly-chilling-spy-network and
https://www.socialcooling.com/

Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications.[115]

33. The Indian government has published a White Paper which provides a comprehensive analysis of the issues and data protection legislation adopted in various jurisdictions, see: http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf

34. All states should have comprehensive data protection legislation.[116] The development of so-called "smart cities" might result in further erosion of individual control of personal data. As one journalist puts the matter[117]: "A close reading [of internal documentation and marketing materials] leaves little room for doubt that vendors ... construct the resident of the smart city as someone without agency; merely a passive consumer of municipal services – at best, perhaps, a generator of data that can later be aggregated, mined for relevant inference, and acted upon." Related issues arise regarding the use of employee data by platforms (such as Uber) that provide so-called "sharing economy" services[118].

35. The same issues arise regarding the replacement of cash payments by various forms of electronic payments. It is important to maintain "alternatives to the stifling hygiene of the digital panopticon being constructed to serve the needs of profit-maximising, cost-minimising, customer-monitoring, control-seeking, behaviour-predicting commercial"[119] companies.

36. Further, mass-collected data (so-called "big data"[120]) are increasingly being used, via computer algorithms, to make decisions that affect people's lives, such as credit rating, availability of insurance, etc.[121] The algorithms used are usually not made public so people's lives are affected by computations made without their knowledge based on data that are often collected without their

[115] See document 2017/0003(COD) of 9 June 2017, available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-606.011%2b01%2bDOC%2bPDF%2bV0%2f%2fEN

[116] See for example p. 42 of GCIG; and section 5 of http://www.itu.int/en/council/cwg-internet/Pages/display-feb2016.aspx?ListItemID=70 . A summary of adoption of data protection and data privacy laws by country can be found at: http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

[117] https://www.theguardian.com/cities/2014/dec/22/the-smartest-cities-rely-on-citizen-cunning-and-unglamorous-technology

[118] See "Stop rampant workplace surveillance" on p. 12 of: http://library.fes.de/pdf-files/id-moe/12797-20160930.pdf

[119] http://thelongandshort.org/society/war-on-cash

[120] An excellent overview of the topic is provided in the May 2014 report commissioned by then-US President Obama, "Big Data: Seizing Opportunities, Preserving Values", available at: https://bigdatawg.nist.gov/pdf/big_data_privacy_report_may_1_2014.pdf . An academic analysis of the social and public interest aspects of big data is given in Taylor, L., Floridi, L., van der Sloot, B. eds. (2017) *Group Privacy: new challenges of data technologies*. Dordrecht: Springer, available at: https://www.stiftung-nv.de/sites/default/files/group-privacy-2017-authors-draft-manuscript.pdf ; see also the analysis and recommendations at: https://medium.com/@AINowInstitute/the-10-top-recommendations-for-the-ai-field-in-2017-b3253624a7

[121] http://time.com/4477557/big-data-biases/?xid=homepage ; an academic discussion is at: http://www.tandfonline.com/doi/full/10.1080/1369118X.2016.1216147 and in the individual articles in:
Information, Communication & Society, Volume 20, Issue 1, January 2017, http://www.tandfonline.com/toc/rics20/20/1

informed consent. An excellent analysis of the human rights dimensions of algorithms is found in Council of Europe document MSI-NET(2016)06[122], which makes a number of recommendations for government actions.

37. It is important to avoid that "big data", and the algorithmic treatment of personal data, do not result in increased inequality[123] and increased social injustice[124] which would threaten democracy.[125] A balanced discussion of the issues in the context of urban centers is given in a well-researched 2017 white paper by CITRIS Connected Communities Initiative.[126] See also the discussion on pp. 75 ff. of the 2017 Internet Society Global Internet Report: Paths to Our Digital Future[127].

38. As learned scholars have put the matter[128]:

> Without people, there is no data. Without data, there is no artificial intelligence. It is a great stroke of luck that business has found a way to monetize a commodity that we all produce just by living our lives. Ensuring we get value from the commodity is not a case of throwing barriers in front of all manner of data processing. Instead, it should focus on aligning public and private interests around the public's data, ensuring that both sides benefit from any deal.
>
> …
>
> A way of conceptualizing our way out of a single provider solution by a powerful first-mover is to think about datasets as public resources, with attendant public ownership interests.

39. Another way of putting it is to note that the use of data is an extractive industry analogous to the mining and oil industries: "No reasonable person would let the mining industry unilaterally decide how to extract and refine a resource, or where to build its mines. Yet somehow we let the tech industry make all these decisions [regarding data] and more, with practically no public oversight. A company that yanks copper out of an earth that belongs to everyone should be governed in everyone's interest. So should a company that yanks data out of every crevice of our collective lives."[129]

[122] https://rm.coe.int/16806a7ccc

[123] https://inequality.org/facts/income-inequality/ and http://wir2018.wid.world/files/download/wir2018-summary-english.pdf

[124] Even a well-known business publication has recognized that there is a need to address the issue of social equality, see: http://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy;
see also pp. 13 and 57 of https://bigdatawg.nist.gov/pdf/big_data_privacy_report_may_1_2014.pdf

[125] See Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown Publishing, 2016; article at: https://www.wired.com/2016/10/big-data-algorithms-manipulating-us/

[126] http://citris-uc.org/wp-content/uploads/2017/07/Inclusive-AI_CITRIS_2017.pdf

[127] https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf

[128] Powles, J. and Hodson, H., Google DeepMind and health care in an age of algorithms, *Health and Technology*, 2017, pp. 1-17, Health Technol. (2017) doi:10.1007/s12553-017-0179-1, available at: http://link.springer.com/article/10.1007%2Fs12553-017-0179-1

[129] https://www.theguardian.com/world/2017/aug/23/silicon-valley-big-data-extraction-amazon-whole-foods-facebook

40. Control of large amounts of data may lead to dominant positions that impeded competition[130]. But such large data sets are valuable only because they combine data from many individuals. Thus the value of the data is derived from the large number of people who contributed to the data. Consequently, "data is an essential, infrastructural good that should belong to all of us; it should not be claimed, owned, or managed by corporations."[131]

41. While some national legislators and/or courts have taken steps to strengthen citizens' rights to control the way their personal data are used[132], to consider product liability issues related to data[133], and to consider the impact of big data with respect to prohibitions of discrimination in hiring[134], there does not appear to be adequate consideration of this issue at the international level.[135] Yet failure to address the issue at the international level can have negative consequences, including for trade. As UNCTAD puts the matter[136]:

> Insufficient protection can create negative market effects by reducing consumer confidence, and overly stringent protection can unduly restrict businesses, with adverse economic effects as a result. Ensuring that laws consider the global nature and scope of their application, and foster compatibility with other frameworks, is of utmost importance for global trade flows that increasingly rely on the Internet.
>
> …
>
> For those countries that still do not have relevant laws in place, governments should develop legislation that should cover data held by the government and the private sector and remove exemptions to achieve greater coverage. A core set of principles appears in the vast majority of national data protection laws and in global and regional initiatives. Adopting this core set of principles enhances international compatibility, while still allowing some flexibility in domestic implementation. Strong support exists for establishing a single central regulator when possible, with a combination of oversight and complaints management functions and powers. Moreover, the trend is towards broadening enforcement powers, as well as increasing the size and range of fines and sanctions in data protection.

[130] https://www.wired.com/story/ai-and-enormous-data-could-make-tech-giants-harder-to-topple/

[131] https://www.theguardian.com/commentisfree/2016/dec/04/data-populists-must-seize-information-for-benefit-of-all-evgeny-morozov

[132] A good academic overview of the issues is found at: http://www.ip-watch.org/2016/10/25/personality-property-data-protection-needs-competition-consumer-protection-law-conference-says/

[133] http://www.wablegal.com/european-commission-publishes-roadmap-future-proof-eu-product-liability-directive/

[134] https://www.eeoc.gov/eeoc/meetings/10-13-16/index.cfm

[135] Indeed, a group of scholars has called for the creation of a charter of digital rights, see: http://www.dw.com/en/controversial-eu-digital-rights-charter-is-food-for-thought/a-36798258 See also the UNCTAD study at: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf; and http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource ; and the balanced discussion in pp. 93-95 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872

[136] *Data protection regulations and international data flows: Implications for trade and development*, pp. xi-xii, available at: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

42. Indeed, the International Conference of Data Protection and Privacy Commissioners has "appealed to the United Nations to prepare a legal binding instrument which clearly sets out in detail the rights to data protection and privacy as enforceable human rights" [137].

43. At its 34th session, 27 February-24 March 2017, the Human Rights Council adopted a new resolution on the Right to privacy in the digital age[138]. That resolution calls for data protection legislation, in particular to prevent the sale of personal data of personal data without the individual's free, explicit and informed consent.[139] We also note that the BRICS Leaders Xiamen Declaration[140] (4 September 2017) stated in its paragraph 13 (emphasis added): "We will advocate the establishment of internationally applicable rules for security of ICT infrastructure, data protection and the Internet that can be widely accepted by all parties concerned, and jointly build a network that is safe and secure."

44. Regarding algorithmic use of data, what a UK parliamentary committee[141] said at the national level can be transposed to the international level:

> After decades of somewhat slow progress, a succession of advances have recently occurred across the fields of robotics and artificial intelligence (AI), fuelled by the rise in computer processing power, the profusion of data, and the development of techniques such a 'deep learning'. Though the capabilities of AI systems are currently narrow and specific, they are, nevertheless, starting to have transformational impacts on everyday life: from driverless cars and supercomputers that can assist doctors with medical diagnoses, to intelligent tutoring systems that can tailor lessons to meet a student's individual cognitive needs.
>
> Such breakthroughs raise a host of social, ethical and legal questions. Our inquiry has highlighted several that require serious, ongoing consideration. These include taking steps to minimise bias being accidentally built into AI systems; ensuring that the decisions they make are transparent; and instigating methods that can verify that AI technology is operating as intended and that unwanted, or unpredictable, behaviours are not produced.

45. A more detailed discussion is given in paragraphs 5-76 of the 19 October 2017 Report of the Special Rapporteur on Privacy.[142]

46. The recommendations of a national artificial intelligence research and development strategic plan[143] can also be transposed at the international level:

[137] https://icdppc.org/wp-content/uploads/2015/02/Montreux-Declaration.pdf
[138] http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/34/L.7/Rev.1
[139] See 5(f) and 5(k) of the cited Resolution
[140] Available at: http://www.mea.gov.in/Uploads/PublicationDocs/28912_XiamenDeclaratoin.pdf
[141] http://www.publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/14502.htm
[142] Document A/72/43103, http://www.ohchr.org/Documents/Issues/Privacy/A-72-43103_EN.docx
[143] https://www.nitrd.gov/news/national_ai_rd_strategic_plan.aspx

> **Strategy 3**: Understand and address the ethical, legal, and societal implications of AI. We expect AI technologies to behave according to the formal and informal norms to which we hold our fellow humans. Research is needed to understand the ethical, legal, and social implications of AI, and to develop methods for designing AI systems that align with ethical, legal, and societal goals.
>
> **Strategy 4**: Ensure the safety and security of AI systems. Before AI systems are in widespread use, assurance is needed that the systems will operate safely and securely, in a controlled, well-defined, and well-understood manner. Further progress in research is needed to address this challenge of creating AI systems that are reliable, dependable, and trustworthy.

47. Indeed members of the European Parliament have called for European rules on robotics and artificial intelligence, in order to fully exploit their economic potential and to guarantee a standard level of safety and security.[144]

48. And experts speaking at a conference[145] on Artificial Intelligence hosted by the ITU raised many of the issues raised in this paper[146], as did experts at the AI Now public symposium, hosted by the White House and New York University's Information Law Institute, July 7th, 2016[147], as did a report by the UK Royal Society[148], as did the Internet Society in pages 31 ff. of its 2017 Global Internet Report: Paths to Our Digital Future[149]. An academic treatment of the issues is given in Wachter, S., Mittelstadt, B., and Floridi, L. (2017) "Transparent, explainable, and accountable AI for robotics", *Science Robotics,* 31 May 2017, Vol. 2, Issue 6, eaan6080, DOI: 10.1126/scirobotics.aan6080[150]. See also pages 4-5 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*[151] and one expert's[152] predictions for 2018.

Recommendation 1

We recommend to invite UNCTAD[153] and UNCITRAL to study the issues related to the economic and social value or data, in particular "big data" and the increasing

[144] See http://www.europarl.europa.eu/news/en/press-room/20170210IPR61808/robots-and-artificial-intelligence-meps-call-for-eu-wide-liability-rules and https://ec.europa.eu/digital-single-market/en/blog/future-robotics-and-artificial-intelligence-europe

[145] http://www.itu.int/en/ITU-T/AI/Pages/201706-default.aspx . The report of the event is at: https://www.slideshare.net/ITU/ai-for-good-global-summit-2017-report

[146] See for example the summary at: https://www.ip-watch.org/2017/06/13/experts-think-ethical-legal-social-challenges-rise-robots/ and http://news.itu.int/enhancing-privacy-security-and-ethics-of-artificial-intelligence/

[147] https://artificialintelligencenow.com/media/documents/AINowSummaryReport_3_RpmwKHu.pdf

[148] https://royalsociety.org/topics-policy/projects/machine-learning/

[149] https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf

[150] http://robotics.sciencemag.org/content/2/6/eaan6080

[151] http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872

[152] https://www.diplomacy.edu/blog/2018predictions#5

[153] For a description of UNCTAD's work addressing related issues, see: http://unctad14.org/EN/pages/NewsDetail.aspx?newsid=31 and in particular: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf ; we also note the newly created Intergovernmental Group of Experts on E-Commerce, see: http://unctad.org/en/Pages/MeetingDetails.aspx?meetingid=1437

use of algorithms (including artificial intelligence[154]) to make decisions[155], which issues include economic and legal aspects. In particular, UNCITRAL should be mandated to develop model laws, and possibly treaties, on personal data protection[156], algorithmic transparency and accountability[157], and artificial intelligence[158]; UNCTAD should be mandated to develop a study on the taxation

[154] For a discussion of some of the issues related to AI, see: https://www.wired.com/2017/02/ai-threat-isnt-skynet-end-middle-class/?mbid=nl_21017_p3&CNDID=42693809 and https://www.technologyreview.com/s/608248/biased-algorithms-are-everywhere-and-no-one-seems-to-care/;
and https://www.technologyreview.com/s/607955/inspecting-algorithms-for-bias/ ; and https://blogs.microsoft.com/blog/2018/01/17/future-computed-artificial-intelligence-role-society/ ;
a good discussion of the issues and some suggestions for how to address them is found at: https://www.internetsociety.org/doc/artificial-intelligence-and-machine-learning-policy-paper

[155] Specific recommendations regarding how to address the issues are found in Section 8, Conclusions and Recommendations, of the September 2016 Council of Europe document "Draft Report on the Human Rights Dimensions of Algorithms" (MSI-NET(2016)06) , available at: https://rm.coe.int/16806a7ccc

[156] Such a model law could flesh out the high-level data security and protection requirements enunciated in 8.7 of Recommendation ITU-T Y.3000, Big data – Cloud computing based requirements and capabilities, available at:
https://www.itu.int/rec/T-REC-Y.3600-201511-I/en; the privacy principles enunciated in 6 of Recommendation ITU-T X.1275, Guidelines on protection of personally identifiable information in the application of RFID technology, available at:
https://www.itu.int/rec/T-REC-X.1275/en; the core principles found in p. 56 and 65 ff. of the cited UNCTAD study at:
http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf; the core principles on page 95 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872;
the core principles enunciated by the Supreme Court of India in paragraph 184 on p. 257 of its recent judgment at:
http://supremecourtofindia.nic.in/pdf/LU/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf ; and the key principles found in Section V of the Indian White Papre (p. 214 of the PDF file, p. 204 of the document) available at:
http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf ;
it should also consider the "Guidelines for the Regulation of Computerized Personal Data Files" adopted by the UN General Assembly resolution 45/95 of 14 December 1990; the Guidelines are at: http://www.refworld.org/pdfid/3ddcafaac.pdf;
the Resolution is at: http://www.un.org/documents/ga/res/45/a45r095.htm.
A treaty could be based on Council of Europe Convention no. 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, available at:
http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37 ; and it could also consider the provisions in Chapter II of the African Union Convention on Cyber Security and Personal Data Protection, available at:
https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf ; and the "Top 10 Principles for Workers' Data Privacy and Protection" published by UNI Global Union, at: http://www.thefutureworldofwork.org/media/35421/uni_workers_data_protection.pdf .
Guidelines/best practices could be based on sections 3-9 of the Council of Europe's T-PD consultative committee's January 2017 *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, available at: https://rm.coe.int/16806ebe7a.

[157] Such a model law/treaty could be flesh out the Principles for Algorithmic Transparency and Accountability published by the Association for Computing Machinery (ACM), see: https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf

[158] Such a model law/treaty could flesh out the Asilomar AI Principles developed by a large number of experts, see:
https://futureoflife.org/ai-principles/ . It should take into account the "Top 10 Principles for Ethical Artificial Intelligence" published by UNI Global Union, at:
http://www.thefutureworldofwork.org/media/35420/uni_ethical_ai.pdf.

of robots[159]; and the UN Conference on Disarmament should consider taking measures with respect to lethal autonomous weapons[160].

2. Takedown, filtering and blocking

49. An increasing number of states have implemented, or are proposing to implement, measures to restrict access to certain types of Internet content[161], e.g. incitement to violence, gambling, copyright violation, or to take measures[162] against individuals who post certain types of content.

50. While such measures are understandable in light of national sensitivities regarding certain types of content, the methods chosen to restrict content must not violate fundamental human rights such as freedom of speech[163], and must not have undesirable technical side-effects.

51. Any restrictions on access to content should be limited to what is strictly necessary and proportionate in a democratic society.[164]

52. At present, there does not appear to be adequate consideration at the international level of how best to conjugate national sensitivities regarding certain types of content with human rights and technical feasibilities.

53. This issue is exacerbated by the fact that certain Internet service providers apply strict rules of their own to content, at times apparently limiting freedom of speech for no good reason.[165]

[159] http://www.bilan.ch/xavier-oberson/taxer-robots; and http://fortune.com/2017/02/18/bill-gates-robot-taxes-automation/; and http://uk.businessinsider.com/bill-gates-robots-pay-taxes-2017-2

[160] A Governmental Group of Experts on this topic has been created, see: https://www.unog.ch/80256EE600585943/(httpPages)/F027DAA4966EB9C7C12580CD0039D7B5?OpenDocument

[161] See the report at: http://www.un.org/ga/search/view_doc.asp?symbol=A/71/373 and the press release at: http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=20717&LangID=E and http://news.sky.com/story/amber-rudd-only-has-google-meetings-planned-as-she-urges-web-extremism-crackdown-10969423 and https://www.bloomberg.com/news/articles/2017-07-10/australia-s-turnbull-urges-internet-providers-to-block-extremism and https://www.diplomacy.edu/blog/2018predictions#7

[162] See for example http://www.cps.gov.uk/news/latest_news/cps_publishes_new_social_media_guidance_and_launches_hate_crime_consultation/ ; and the summary article at: https://techcrunch.com/2016/10/12/ai-accountability-needs-action-now-say-uk-mps/

[163] See the report cited above, A/71/373 and paragraph 49 of A/HRC/35/22 at http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/35/22

[164] See in this respect the 30 March 2017 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, document A/HRC/35/22. At http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/35/22

[165] See for example https://www.theguardian.com/technology/2016/sep/09/facebook-deletes-norway-pms-post-napalm-girl-post-row

Recommendation 2

Since the right of the public to correspond by telecommunications is guaranteed by Article 33 of the ITU Constitution (within the limits outlined in Article 34), we recommend to invite IETF, ITU, OHCHR, and UNESCO jointly to study the issue of takedown, filtering, and blocking, which includes technical, legal, and ethical aspects.

3. Intermediary liability

54. The issue of the extent to which Internet service providers, and other intermediaries such as providers of online video content, are or should be liable for allowing access to illegal material has been addressed by many national legislators.[166]

55. However, there does not appear to be adequate consideration of this issue at the international level.[167]

Recommendation 3

We recommend to invite UNCITRAL to study the issue of intermediary liability, with a view to proposing a model law on the matter[168].

4. Privacy, encryption and prevention of inappropriate mass surveillance

56. Privacy is a fundamental right, and any violation of privacy must be limited to what is strictly necessary and proportionate in a democratic society.[169] Certain states practice mass surveillance that violates the right to privacy[170] (see for example A/HRC/31/64[171], A/71/373[172], A/HRC/34/60[173] and European Court of Justice judgment[174] ECLI:EU:C:2016:970 of 21 December 2016). As noted by the UN Human Rights Council Special Rapporteur on the promotion and

[166] https://cyberlaw.stanford.edu/our-work/projects/world-intermediary-liability-map-wilmap ; see also 17-23 of a European Parliament Committee Report on online platforms and the digital single market, (2016/2276(INI): http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-599.814+01+DOC+PDF+V0//EN&language=EN

[167] We note however the civil society initiative resulting in the Manila Principles, see: https://www.manilaprinciples.org/

[168] In this context, consideration should be given to the Geneva Internet Dispute Resolution Policies, see: https://geneva-internet-disputes.ch/

[169] See for example pp. vii, 32, 106 and 133 of GCIG; and 3(H) on p. 264 of the recent judgment of the Supreme Court of India, at http://supremecourtofindia.nic.in/pdf/LU/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf

[170] For an academic discussion, see http://dx.doi.org/10.1080/23738871.2016.1228990 and http://ijoc.org/index.php/ijoc/article/view/5521/1929 and the articles at http://ijoc.org/index.php/ijoc/issue/view/13

[171] http://ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc

[172] http://www.un.org/ga/search/view_doc.asp?symbol=A/71/373

[173] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session34/Documents/A_HRC_34_60_EN.docx; see in particular paragraphs 13-15, 18, 25 **and especially 42**.

[174] http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&doclang=EN ; for a summary of the judgement, see: http://www.commondreams.org/news/2016/12/21/eus-top-court-delivers-major-blow-mass-surveillance

protection of the right to freedom of opinion and expression, this can have negative effects on freedom of speech.[175] The UN Human Rights Council Special Rapporeur on the right to privacy stated that he had "identified a serious obstacle to privacy in that there is a vacuum in international law in surveillance and privacy in cyberspace. ... It is not only the lack of substantive rules which are an obstacle to privacy promotion and protection, but also one of adequate mechanisms."[176] He also stated that the UN should discuss and adopt a new instrument to protect privacy rights.[177]

57. As UNCTAD puts the matter[178]:

> countries need to implement measures that place appropriate limits and conditions on surveillance. Key measures that have emerged include:
>
> - providing a right to legal redress for citizens from any country whose data is transferred into the country (and subject to surveillance);
> - personal data collection during surveillance should be 'necessary and proportionate' to the purpose of the surveillance; and
> - surveillance activities should be subject to strong oversight and governance.

58. At its 34th session, 27 February-24 March 2017, the Human Rights Council (HRC) adopted a new resolution on the Right to privacy in the digital age[179]. That resolution recalls that States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality.[180] Even a well-known business publication has recognized that privacy is a pressing issue[181]. And many of the issued mentioned in this contribution have been well presented in the 27 July 2017 Issue Paper "Online Privacy" of the Internet Society Asia-Pacific Bureau.[182]

59. The President of the United States has promulgated an Executive Order titled Enhancing Public Safety in the Interior of the United States. Its section 14 reads: "Privacy Act. Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."[183]

[175] See paragraphs 17, 21, 22 and 78 of A/HRC/35/22 at http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/35/22

[176] Paragraph 4 of the 19 October 2017 Report of the Special Rapporteur on Privacy, document A/72/43103, http://www.ohchr.org/Documents/Issues/Privacy/A-72-43103_EN.docx

[177] Paragraph 5 of the cited report.

[178] *Data protection regulations and international data flows: Implications for trade and development*, p. 66, available at: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

[179] http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/34/L.7/Rev.1

[180] See 2 of the cited HRC Resolution

[181] http://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy

[182] https://www.internetsociety.org/doc/issue-paper-asia-pacific-bureau-%E2%80%93-online-privacy

[183] https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united

60. It appears to us that this decision and questions[184] related to its impact highlight the need to reach international agreement on the protection of personal data.

61. The same holds for a recent public admission that the agencies of at least one state monitor the communications of at least some accredited diplomats, even when the communications are with a private person ("... intelligence and law enforcement agencies ... routinely monitor the communications of [certain] diplomats" [185]). Surely there is a need to agree at the international level on an appropriate level of privacy protection for communications.

62. Encryption is a method that can be used by individuals to guarantee the secrecy of their communications. Some states have called for limitations on the use of encryption[186], or for the implementation of technical measures to weaken encryption. Many commentators have pointed out that any weakening of encryption can be exploited by criminals and will likely have undesirable side effects (see for example paragraphs 42 ff. of A/HRC/29/32[187]). Many commentators oppose state-attempts to compromise encryption.[188] The 2016 UNESCO Report "Human rights and encryption" also points out that attempts to limit the use of encryption, or to weaken encryption methods, may impinge on freedom of expression and the right to privacy.[189] The cited HRC resolution calls on states not to interfere with the use of encryption.[190] The Internet Society recommends the following[191]: "Encryption is and should remain an integral part of the design of Internet technologies, applications and services. It should not be seen as a threat to security. We must strengthen encryption, not weaken it." And this because "If governments persist in trying to prevent the use of encryption, they put at risk not only freedom of expression, privacy, and user trust, but the future Internet economy as well."[192]

63. At present, most users do not use encryption for their E-Mail communications, for various reasons, which may include lack of knowledge and/or the complexity of implementing encryption. There is a general need to

[184] See for example: http://www.sophieintveld.eu/letter-to-eu-commission-what-impact-has-trump-decisions-on-privacy-shield-and-umbrella-agreement/

[185] https://www.washingtonpost.com/world/national-security/national-security-adviser-flynn-discussed-sanctions-with-russian-ambassador-despite-denials-officials-say/2017/02/09/f85b29d6-ee11-11e6-b4ff-ac2cf509efe5_story.html?utm_term=.63a87203f039

[186] See for example https://www.bloomberg.com/news/articles/2017-07-10/australia-s-turnbull-urges-internet-providers-to-block-extremism and https://www.diplomacy.edu/blog/2018predictions#9

[187] https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement

[188] See for example pp. vii, 106, and 113 of GCIG. See also http://science.sciencemag.org/content/352/6292/1398; http://www.internetsociety.org/policybriefs/encryption; section 4 of http://www.itu.int/en/council/cwg-internet/Pages/display-feb2016.aspx?ListItemID=70 ; https://securetheinternet.org/ and http://dl.cryptoaustralia.org.au/Coalition+Letter+to+5eyes+Govs.pdf

[189] See in particular pp. 54 ff. The Report is at: http://unesdoc.unesco.org/images/0024/002465/246527e.pdf

[190] See 9 of the cited HRC Resolution

[191] Page 106 of the 2017 Global Internet Report: Paths to Our Digital Future, available at: https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf

[192] Page 39 of the cited ISOC report.

increase awareness of ways and means for end-users to improve the security of the systems they use.[193]

64. Secrecy of telecommunications is guaranteed by article 37 of the ITU Constitution. However, this provision appears to be out of date and to require modernization[194]. In particular, restrictions must be placed on the collection and aggregation of meta-data.[195]

65. There does not appear to be adequate consideration of the issues outlined above at the international level.[196]

Recommendation 4

We recommend to invite IETF, ISOC, ITU, and OHCHR[197] to study the issues of privacy, encryption and prevention of inappropriate mass surveillance, which include technical, user education, and legal aspects.

5. Internet of Things (IoT)

66. In the current environment, it can be expected that networked devices (the so-called Internet of Things – IoT)[198] will transmit data to manufacturers and service providers with little or no restrictions on the use of the data. [199] The recipients of the data could then correlate the data and resell it, as is currently the case for data collected by so-called free services such as search engines. Further, national surveillance programs could acquire such data and use it to construct profiles of individuals.

67. Such uses of data that are collected automatically for a specific purpose could have wide-reaching and unforeseen consequences.[200]

68. Further, interconnected devices may make decisions affecting daily life,[201] and this may call for the development of a regulatory framework to

[193] See for example p. 66 of GCIG; and https://www.internetsociety.org/blog/2017/10/krack-reinforces-need-encryption-multiple-layers-stack/

[194] For a specific proposal, see the last page of the proposals at: https://justnetcoalition.org/sites/default/files/HCHR_report_final.pdf

[195] See p. 31 of GCIG.

[196] See paragraph 46 of http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session34/Documents/A_HRC_34_60_EN.docx

[197] We note with gratitude that the Human Rights Council Special Rapporteur on Privacy has initiated work on a possible international legal instrument on surveillance, see: http://www.ohchr.org/Documents/Issues/Privacy/SurveillanceAndPrivacy.doc and http://www.ohchr.org/Documents/Issues/Privacy/DraftLegalInstrumentGovernmentLed.pdf

[198] A good overview of the technology, and the issues it raises, can be found at: http://www.internetsociety.org/doc/iot-overview ; a more detailed account is at: http://www.gao.gov/assets/690/684590.pdf

[199] See https://www.theguardian.com/technology/2015/jul/15/internet-of-things-mass-surveillance and the articles it references.

[200] See for example: http://www.itu.int/en/ITU-T/Workshops-and-Seminars/01072016/Documents/S1P3_Corinna_Schmitt_v3.pdf ; see also the "weaponization of everything", see p. 2 of GCIG.

[201] http://policyreview.info/articles/analysis/governance-things-challenge-regulation-law

protect the interests of citizens. In particular, the issue of product liability may require changes to existing legal regimes.[202]

69. Increasingly, the safety of IoT devices will be affected by their security.[203] Thus, the security risks[204] posed by interconnected devices may require government actions.[205] For example, there may be a need to provide incentives to those who make interconnected devices to make them secure: such incentives might be penalties for failure to build-in adequate security[206]. In this context, it is worth considering past experience with various devices, including electrical devices: they all have to conform to legal standards, all countries enforce compliance with such standards. It is not legitimate to claim that security and safety requirement stifle technological innovation. It must be recalled that the primary goal of private companies is to maximize profits. The purpose of regulation is to prevent profit-maximization from resulting in the production of dangerous products. As IBM Resilient Chief Technology Officer Bruce Schneier puts the matter[207], cybersecurity risks associated with the IoT require governmental intervention, as "the market is not going to fix this because neither the buyer nor the seller cares".

[202] http://www.wablegal.com/european-commission-publishes-roadmap-future-proof-eu-product-liability-directive/

[203] https://www.iottechnews.com/news/2017/aug/04/why-iot-security-so-important-and-what-do-about-it/;
and http://www.cl.cam.ac.uk/~rja14/Papers/weis2017.pdf and
pages 5-6 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872 . A very good overview is given on p. 115 of ITU, Measuring the Information Society Report 2017, Vol. 1, at: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf and 2017 ENISA Baseline Security Recommendations for IoT at: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot . For a comprehensive analysis, see the draft Report to the US President "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats" at:
https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf

[204] http://about.att.com/story/iot_cybersecurity_alliance.html ; see also http://www.businesswire.com/news/home/20170313005114/en/Tripwire-Study-96-Percent-Security-Professionals-Expect ; and pages 46 ff. and 73 of the Internet Society 2017 Global Internet Report: Paths to Our Digital Future, available at https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf

[205] https://www.schneier.com/blog/archives/2016/07/real-world_secu.html and
https://www.scribd.com/document/328854049/DDoS-Letter-to-Chairman-Wheeler#download and
https://www.euractiv.com/section/innovation-industry/news/commission-plans-cybersecurity-rules-for-internet-connected-machines/ and
http://www.dailydot.com/layer8/bruce-schneier-internet-of-things/ and
https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity and section section 6.2 of the 2017 ENISA Baseline Security Recommendations for IoT at:
https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot and the ISOC paper "IoT Security for Policymakers" (forthcoming).
For an academic discussion, see pp. 4 ff. of:
https://www.ntia.doc.gov/files/ntia/publications/k_farhat_ntia_iot.pdf

[206] http://www.wablegal.com/european-commission-publishes-roadmap-future-proof-eu-product-liability-directive/. In the USA, the Federal Trade Commission (FTC) has invoked general consumer protection law to fine companies that do not have adequate online security, see *Wyndham vs. FTC*, at: http://www2.ca3.uscourts.gov/opinarch/143514p.pdf

[207] https://digitalwatch.giplatform.org/updates/new-government-agencies-are-needed-deal-iot-security-regulations-says-ibm-resilient-cto and
http://searchsecurity.techtarget.com/news/450413107/Bruce-Schneier-Its-time-for-internet-of-things-regulation

70. Since IoT products will be interconnected, at least to some degree, chaos can ensue if the products are not sufficiently secure[208] (e.g. all medical systems fail to work). Thus it is important to ensure that the products are sufficiently secure for mass deployment.

71. This is not a theoretical consideration. Insufficiently insecure IoT devices have already been used to perpetrate massive denial of service attacks, and such attacks could be used to bring down critical infrastructures.[209] As one security manager put the matter[210]: "In a relatively short time we've taken a system built to resist destruction by nuclear weapons and made it vulnerable to toasters." A thorough study of the matter, which identifies gaps and contains recommendations for remedial actions, was published on 8 February 2017 by ENISA, see: https://www.enisa.europa.eu/publications/m2m-communications-threat-landscape

72. In the US, a law[211] has been proposed to that would set minimum security standards for the government's purchase and use of a broad range IoT devices.[212] Related proposals are found in a draft report to the US President.[213]

73. But ICTs in general, and the Internet in particular, are global phenomena, so minimum security standards must also be global (or at least importing products that don't comply with internationally agreed standards should be prohibited), otherwise there will be a race to produce products in jurisdictions that don't have minimum security standards.

74. As a draft Report to the US President puts the matter[214]:

> Significant enhancements to the resilience of the ecosystem cannot be achieved through domestic action alone. The United States should lead engagement with international partners through regular bilateral and multilateral engagements on cybersecurity by leveraging expertise within the federal D/As. …
>
> …
>
> International standardization could be particularly beneficial. Widely applicable international standards for IoT security could expand the

[208] A particularly frightening scenario is presented at: https://www.schneier.com/blog/archives/2016/11/self-propagatin.html

[209] See http://hothardware.com/news/latest-iot-ddos-attack-dwarfs-krebs-takedown-at-nearly-1-terabyte-per-second
http://hothardware.com/news/your-iot-device-could-be-part-of-a-ddos-botnet-how-to-shut-it-down
https://www.schneier.com/blog/archives/2016/09/someone_is_lear.html

[210] Jeff Jarmoc, head of security for global business service Salesforce, quoted in the excellent summary article at: http://www.bbc.com/news/technology-37738823

[211] https://www.scribd.com/document/355269230/Internet-of-Things-Cybersecurity-Improvement-Act-of-2017

[212] https://krebsonsecurity.com/2017/08/new-bill-seeks-basic-iot-security-standards/

[213] See Section III, Actions 1.2 and 1.4 at: https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf

[214] Section III, Action 4.2 at: https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf

> market for products that contribute to the resilience of the ecosystem while leveling the playing field for American businesses. As the NSTAC report recommended, industry and federal agencies that participate in standards development should coordinate on a strategy for engaging within appropriate industry-driven international standards bodies to ensure U.S. representation and leadership, and through that participation, champion a flexible and interoperable suite of international standards for IoT security.

75. At present, there does not appear to be adequate consideration of this issue at the international level.

Recommendation 5

We recommend to invite ITU, UNCITRAL and UNESCO to study issues related to IoT (including security of IoT devices, use of data from IoT devices, decisions made by IoT devices, etc.), which include technical, legal, and ethical aspects (for a partial list of such aspects, see Recommendation ITU-T Y.3001: Future networks: Objectives and design goals[215]). The studies should take into account Recommendation ITU-T Y.3013: Socio-economic assessment of future networks by tussle analysis[216] as well as work in other bodes, in particular IEEE[217] and ENISA[218].

6. Externalities arising from lack of security and how to internalize such externalities

76. Security experts have long recognized that lack of ICT security creates a negative externality.[219] For example, if an electronic commerce service is hacked and credit card information is disclosed, the users of the service users will have to change their credit cards. This is a cost both for the user and for the credit card company. But that cost is not visible to the electronic commerce service. Consequently, the electronic commerce service does not have an incentive to invest in greater security measures.[220] Another, very concrete, example is provided by a software manufacturer's decision to stop correcting security problems in old versions of its software, with the consequence that a large number of computers were affected.[221] The cost of the attack was borne by the end-users, not by the software manufacturer.

77. As the Global Internet Report 2016 of the Internet Society puts the matter[222]:

[215] https://www.itu.int/rec/T-REC-Y.3001-201105-I

[216] http://www.itu.int/rec/T-REC-Y.3013-201408-I/en

[217] http://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_may_2017.pdf

[218] https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[219] https://www.schneier.com/blog/archives/2007/01/information_sec_1.html ; a comprehensive discussion is given in pages 103-107 of the Global Internet Report 2016 of the Internet Society, see in particular the examples on p. 101. The Report is available at: https://www.internetsociety.org/globalinternetreport/2016/ . See also item 5 on page 8 of: https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf

[220] See also pp. vii and 66 of GCIG.

[221] https://en.wikipedia.org/wiki/WannaCry_cyber_attack

[222] See p. 18 of the cited Global Internet Report 2016.

> There is a market failure that governs investment in cybersecurity. First, data breaches have externalities; costs that are not accounted for by organisations. Second, even where investments are made, as a result of asymmetric information, it is difficult for organizations to convey the resulting level of cybersecurity to the rest of the ecosystem. As a result, the incentive to invest in cybersecurity is limited; organisations do not bear all the cost of failing to invest, and cannot fully benefit from having invested.

78. There can be little doubt that many organizations are not taking sufficient measures to protect the security of their computer systems, see for example the May 2017 attack[223] that affected a large number of users and many hospitals.

79. As the European Union Agency for Network and Information Security (ENISA) puts the matter[224]: "Today we are seeing a **market failure for cybersecurity and privacy**: trusted solutions are more costly for suppliers and buyers are reluctant to pay a premium for security and privacy" (emphasis in original).

80. As noted above, the externalities arising from lack of security are exacerbated by the Internet of Things (IoT)[225]. As a well known security expert puts the matter[226]: "Security engineers are working on technologies that can mitigate much of this risk, but many solutions won't be deployed without government involvement. This is not something that the market can solve. ... the interests of the companies often don't match the interests of the people. ... Governments need to play a larger role: setting standards, policing compliance, and implementing solutions across companies and networks."

81. Recent research shows that a perceived lack of security is reducing consumer propensity to use the Internet for certain activities.[227]

82. Some national authorities are taking some measures.[228] In particular, the President of the USA issued an Executive Order[229] on 11 May 2017 that states:

[223] https://en.wikipedia.org/wiki/WannaCry_cyber_attack

[224] Preamble of https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity

[225] See p. 107 of the cited Global Internet Report 2016.

[226] https://www.schneier.com/blog/archives/2016/07/real-world_secu.html

[227] https://www.cigionline.org/internet-survey ; and pages 22 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872

[228] For example, for cybersecurity for motor vehicles, see: http://www.nhtsa.gov/About-NHTSA/Press-Releases/nhtsa_cybersecurity_best_practices_10242016 . For a general approach see Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[229] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, available at: https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

> [certain high officials will lead] an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the internet [sic] and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets).
> ...
>
> As a highly connected nation, the United States is especially dependent on a globally secure and resilient internet [sic] and must work with allies and other partners toward maintaining the policy set forth in this section.

ENISA is recommending[230] the development of "So called **baseline requirements** for IoT security and privacy that cover the essentials for trust, e.g. rules for authentication / authorization, should set **mandatory reference levels for trusted IoT solutions**." And it is recommending that the European Commission encourage "**the development of mandatory staged requirements for security and privacy in the IoT, including some minimal requirements.**" (Emphases in original)

83. Despite those national or regional initiatives, at present, there does not appear to be adequate consideration of these issues at either the national (in many countries) or international levels. In June 2016, German Chancellor Merkel called[231] for international regulations for digital markets, and in particular for international standards and rules for security; and one expert[232] predicts that the topic will get increasing attention in 2018.

Recommendation 6.1

We recommend to invite IETF, ISOC, ITU, UNCITRAL, and UNCTAD to study the issue of externalities arising from lack of security, which has technical, economic, and legal aspects. In particular, UNCITRAL should be mandated to develop a model law on the matter.

84. Further, as stated by the President of a leading software company (Microsoft)[233]:

> The time has come to call on the world's governments to come together, affirm international cybersecurity norms that have emerged in recent years, adopt new and binding rules and get to work implementing them. In short, the time has come for governments to adopt a Digital Geneva Convention to protect civilians on the internet.
> …
>
> … governments around the world should pursue a broader multilateral agreement that affirms recent cybersecurity norms as global rules. Just

[230] Sections 2.1 and 2.3 of https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity

[231] http://www.rawstory.com/2017/06/germanys-merkel-says-digital-world-needs-global-rules/

[232] https://www.diplomacy.edu/blog/2018predictions#2

[233] https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.00017arazqit2faipqq2lyngzmxx4

> as the world's governments came together in 1949 to adopt the Fourth Geneva Convention to protect civilians in times of war, we need a Digital Geneva Convention that will commit governments to implement the norms that have been developed to protect civilians on the internet in times of peace.
>
> Such a convention should commit governments to avoiding cyber-attacks that target the private sector or critical infrastructure or the use of hacking to steal intellectual property. Similarly, it should require that governments assist private sector efforts to detect, contain, respond to and recover from these events, and should mandate that governments report vulnerabilities to vendors rather than stockpile, sell or exploit them.
>
> In addition, a Digital Geneva Convention needs to create an independent organization that spans the public and private sectors. Specifically, the world needs an independent organization that can investigate and share publicly the evidence that attributes nation-state attacks to specific countries.
>
> While there is no perfect analogy, the world needs an organization that can address cyber threats in a manner like the role played by the International Atomic Energy Agency in the field of nuclear non-proliferation. This organization should consist of technical experts from across governments, the private sector, academia and civil society with the capability to examine specific attacks and share the evidence showing that a given attack was by a specific nation-state. Only then will nation-states know that if they violate the rules, the world will learn about it.

In a press conference on 11 May 2017[234], the official presenting the cited US Executive Order[235] stated:

> ... I think the [security] trend is going in the wrong direction in cyberspace, and it's time to stop that trend .... We've seen increasing attacks from allies, adversaries, primarily nation states but also non-nation state actors, and sitting by and doing nothing is no longer an option.
>
> ...
>
> ... [several] nation states are motivated to use cyber capacity and cyber tools to attack our people and our governments and their data. And that's something that we can no longer abide. We need to establish the rules of the road for proper behavior on the Internet, but we also then need to deter those who don't want to abide by those rules.

[234] https://www.whitehouse.gov/the-press-office/2017/05/11/press-briefing-principal-deputy-press-secretary-sarah-sanders-and

[235] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, available at: https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

Following the WannaCrypt attack[236] in mid-May 2017, Microsoft reinforced its call for action, stating[237]:

> Finally, this attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem. This is an emerging pattern in 2017. We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world. Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage. An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen. And this most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats in the world today – nation-state action and organized criminal action.
>
> The governments of the world should treat this attack as a wake-up call. They need to take a different approach and adhere in cyberspace to the same rules applied to weapons in the physical world. We need governments to consider the damage to civilians that comes from hoarding these vulnerabilities and the use of these exploits. This is one reason we called in February for a new "Digital Geneva Convention" to govern these issues, including a new requirement for governments to report vulnerabilities to vendors, rather than stockpile, sell, or exploit them.

85. Civil society organizations have also called for treaty provisions to ensure that the Internet is used only for peaceful purposes.[238] A knowledgeable expert has explained the historical context for treaty-level provisions regarding cybersecurity.[239]

86. Indeed there is a long history of telecommunications (and by extension digital and cyber) security public international law since 1850, embodied in treaty instruments developed by the signatory nations of what is now known as the International Telecommunication Union (ITU), see: http://www.emeraldinsight.com/doi/abs/10.1108/14636691111101856

[236] https://en.wikipedia.org/wiki/WannaCry_cyber_attack

[237] https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#sm.00017arazqit2faipqq2lyngzmxx4 ; see also: https://www.wired.com/2017/05/microsoft-right-need-digital-geneva-convention/

[238] See point 5 of the Delhi Declaration, at https://justnetcoalition.org/delhi-declaration ; see also http://twn.my/title2/resurgence/2017/319-320/cover08.htm

[239] http://www.circleid.com/posts/20180108_china_pursuit_of_public_international_cybersecurity_law_leadership/

Recommendation 6.2

We recommend to invite the UN General Assembly to consider the appropriate ways and means to convene a treaty-making conference to develop and adopt a binding treaty on norms to protect civilians against cyber-attacks, in particular on the Internet, in times of peace, and to consider whether to develop a new treaty, or whether to invite the ITU to integrate such norms into its own instruments, for example the International Telecommunication Regulations.

7. Ethical issues of networked automation, including driverless cars

87. More and more aspects of daily life are controlled by automated devices, and in the near future automated devices will provide many services that are today provided manually, such as transportation. Automated devices will have to make choices and decisions.[240] It is important to ensure that the choices and decisions comply with our ethical values. In this context, it is worrisome that some modern AI algorithms cannot be understood, to the point where it might be impossible to find out why an automated car malfunctioned[241].

88. According to one analysis, the new European Union Data Protection Regulation "will restrict automated individual decision-making (that is, algorithms that make decisions based on user-level predictors) which 'significantly affect' users. The law will also create a 'right to explanation,' whereby a user can ask for an explanation of an algorithmic decision that was made about them." [242] See also the discussion of algorithmic data processing and artificial intelligence presented under item 1 above.

89. At present, some actions have been proposed at the national level[243], but there does not appear to be adequate consideration of these issues at the international level.

[240] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//EN

[241] https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/

[242] http://arxiv.org/abs/1606.08813

[243] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//EN and http://wam.ae/en/details/1395302639203

Recommendation 7

We recommend to invite UNESCO and UNICTRAL to study the ethical issues of networked automation, including driverless cars, which include ethical and legal aspects.[244] As a starting point, the study should consider the IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems. *Ethically Aligned Design: A Vision For Prioritizing Wellbeing With Artificial Intelligence And Autonomous Systems*, Version 1. IEEE, 2016[245]; and the recommendations of the AI Now 2017 Report[246].

8. How to deal with induced job destruction and wealth concentration

90. Scholars have documented the reduction in employment that has already been caused by automation[247]. It is likely that this trend will be reinforced in the future.[248] Even if new jobs are created as old jobs are eliminated, the qualifications for the new jobs are not the same as the qualifications for the old jobs.[249] And artificial intelligence can even result in the elimination of high-

[244] A commission of the European Parliament "Strongly encourages international cooperation in setting regulatory standards under the auspices of the United Nations" with respect to these issues, see 33 of the draft report cited in the previous footnote. See also: http://www.thedrive.com/tech/11241/audi-ceo-calls-for-discussion-of-self-driving-car-ethics-at-united-nations-summit and https://www.ip-watch.org/2017/06/13/experts-think-ethical-legal-social-challenges-rise-robots/ and http://news.itu.int/enhancing-privacy-security-and-ethics-of-artificial-intelligence/

[245] http://standards.ieee.org/develop/indconn/ec/autonomous_systems.html ; see also: https://www.ip-watch.org/2017/11/27/new-standards-projects-ieee-ethics-autonomous-intelligent-systems/

[246] https://ainowinstitute.org/AI_Now_2017_Report.pdf

[247] Paradoxically, automation has not increased productivity as much as would have been expected, and consequently it has resulted in stagnation of wages for most people and increasing income inequality, see: https://www.technologyreview.com/s/608095/it-pays-to-be-smart/

[248] http://robertmcchesney.org/2016/03/01/people-get-ready-the-fight-against-a-jobless-economy-and-a-citizenless-democracy/ and http://www.newsclick.in/international/review-schiller-dan-2014-digital-depression-information-technology-and-economic-crisis and p. 88 of GCIG and http://library.fes.de/pdf-files/wiso/12864.pdf and http://library.fes.de/pdf-files/wiso/12866.pdf and http://unctad.org/en/PublicationsLibrary/presspb2016d6_en.pdf and https://www.technologyreview.com/s/602869/manufacturing-jobs-arent-coming-back/ and http://www.other-news.info/2017/03/the-robots-are-coming-your-jobs-are-at-risk/ and https://www.nytimes.com/2017/03/28/upshot/evidence-that-robots-are-winning-the-race-for-american-jobs.html?_r=0 and https://blogs.microsoft.com/blog/2018/01/17/future-computed-artificial-intelligence-role-society/ and https://hackernoon.com/artificial-intelligence-3c6d80072416 .
While not necessarily related to ICTs, it is worrisome that the economic situation of least developed countries is deteriorating, see: http://unctad.org/en/PublicationsLibrary/ldc2016_en.pdf; a balanced discussion of the issues is given in pp. 63 ff. of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872

[249] See for example p. viii of GCIG; see also http://www.economist.com/news/leaders/21701119-what-history-tells-us-about-future-artificial-intelligenceand-how-society-should; and https://www.technologyreview.com/s/601682/dear-silicon-valley-forget-flying-cars-give-us-economic-growth/; https://www.technologyreview.com/s/602489/learning-to-prosper-in-a-factory-town/: and http://www.other-news.info/2017/01/poor-darwin-robots-not-nature-now-make-the-selection/ and http://www.pwc.co.uk/services/economics-policy/insights/uk-economic-outlook.html and http://www.pwc.co.uk/economic-services/YWI/pwc-young-workers-index-2017-v2.pdf and http://www.worldbank.org/en/publication/wdr2016

skilled jobs[250], including creation of software[251]. These developments, including the so-called sharing economy, pose policy and regulatory challenges[252], in particular for developing countries[253]. As the Internet Society puts the matter on page 35 of its 2017 Global Internet Report: Paths to Our Digital Future[254]: "The benefits of AI may also be unevenly distributed: for economies that rely on low-skilled labour, automation could challenge their competitive advantage in the global labour market and exacerbate local unemployment challenges, impacting economic development." See also the discussion on page 66 ff. of the cited report.

91. Further, it has been observed that income inequality[255] is increasing in most countries, due at least in part to the deployment of ICTs[256]. More broadly, it is important to consider the development of ICTs in general, and the Internet in particular, from the point of view of social justice[257]. Indeed, it has been posited that the small number of individuals who control the wealth generated by dominant platforms (see below) may be using that wealth to further particular economic and political goals, and that such goals may erode social justice.[258] Further, the algorithms that are increasingly used to automate

[250] https://www.technologyreview.com/s/603431/as-goldman-embraces-automation-even-the-masters-of-the-universe-are-threatened/

[251] https://www.technologyreview.com/s/603381/ai-software-learns-to-make-ai-software/

[252] See for example p. 89 of GCIG. And the recent call for doing more to help globalization's losers by Mario Draghi, the president if the European Central Bank, Donald Tusk, the president of the European Council, and Christine Lagarde, the head of the International Monetary Fund, reported in the Financial Times: https://www.ft.com/content/ab3e3b3e-79a9-11e6-97ae-647294649b28 ; see also
http://twn.my/title2/resurgence/2017/319-320/cover04.htm
http://twn.my/title2/resurgence/2017/319-320/cover05.htm
http://twn.my/title2/resurgence/2017/319-320/cover06.htm and Recommendation 2 of:
https://artificialintelligencenow.com/media/documents/AINowSummaryReport_3_RpmwKHu.pdf ; and pp. 50-51 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872.
The legal issues are well summarized in the 4 April 2017 report of the International Bar Association "Artificial Intelligence and Robotics and Their Impact on the Workplace", available at:
https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=012a3473-007f-4519-827c-7da56d7e3509

[253] See for example http://twn.my/title2/resurgence/2017/319-320/cover01.htm and the UNCTAD Policy Brief No. 50 of October 2016 at
http://unctad.org/en/PublicationsLibrary/presspb2016d6_en.pdf

[254] https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf

[255] See for example https://www.oxfam.org/en/research/working-few ;
https://www.oxfam.org/en/research/economy-99
https://inequality.org/facts/income-inequality/

[256] See for example pp. 14, 20-21, and 118 ff. of the World Bank's 2016 Word Development Report (WDR-2016), titled "Digital Dividends", available at:
http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf

[257] By "social justice" we mean the fair and just relation between the individual and society. This is measured by the explicit and tacit terms for the distribution of wealth, opportunities for personal activity and social privileges. See https://en.wikipedia.org/wiki/Social_justice;
a thorough discussion of the issues (impact on jobs, impact on income inequality, etc.), with many references, is found at: http://www.truth-out.org/news/item/40495-the-robot-economy-ready-or-not-here-it-comes.

[258] http://www.commondreams.org/news/2016/01/20/just-who-exactly-benefits-most-global-giving-billionaires-bill-gates and
http://www.thedailybeast.com/articles/2016/08/11/today-s-tech-oligarchs-are-worse-than-the-robber-barons.html .
A cogent analysis, which points out that the redistribution issues are global and not merely national (because nations that are advanced in terms of automation and artificial intelligence will reap the greatest economic benefits) is given at:
https://www.nytimes.com/2017/06/24/opinion/sunday/artificial-intelligence-economic-inequality.html

decisions such as granting home loans may perpetuate or even increase inequality and social injustice.[259]

92. At present, there does not appear to be adequate consideration of these issues at the international level, even if ILO[260] has recently started to address some of the issues.

Recommendation 8
We recommend to invite ILO and UNCTAD to study the issues of induced job destruction, wealth concentration, and the impact of algorithms on social justice and that UNCTAD compile and coordinate the studies made by other agencies such as OECD, World Bank, IMF.

9. How to deal with platform dominance

93. It is an observed fact that, for certain specific services (e.g. Internet searches, social networks, online book sales, online hotel reservations) one particular provider becomes dominant[261]. If the dominance is due to a better service offer, then market forces are at work and there is no need for regulatory intervention.

94. But if the dominance is due to economies of scale and network effects[262], then a situation akin to a natural monopoly[263] might arise, there might be abuse of dominant market power[264], and regulatory intervention is required[265]. For

[259] https://www.fordfoundation.org/ideas/equals-change-blog/posts/weapons-of-math-destruction-data-scientist-cathy-o-neil-on-how-unfair-algorithms-perpetuate-inequality/

[260] http://www.other-news.info/2017/04/humanity-and-social-justice-a-must-for-the-future-of-work-ryder/ and http://ilo.org/global/topics/future-of-work/WCMS_569528/lang--en/index.htm

[261] https://www.technologyreview.com/s/607954/why-tesla-is-worth-more-than-gm/ and https://www.technologyreview.com/s/608095/it-pays-to-be-smart/

[262] Which is in fact the case for many dominant providers of services on the Internet, see: https://www.technologyreview.com/s/607954/why-tesla-is-worth-more-than-gm/ and https://www.technologyreview.com/s/608095/it-pays-to-be-smart/ ; see also pages 9 and 12 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872

[263] https://en.wikipedia.org/wiki/Natural_monopoly

[264] https://newint.org/features/2016/07/01/smiley-faced-monopolists/ ; and the more radical criticism at: http://www.rosalux-nyc.org/wp-content/files_mf/scholz_platformcoop_5.9.2016.pdf ; specific criticism of a dominant online retailer is at: http://www.truth-out.org/news/item/38807-1-of-every-2-spent-online-goes-to-amazon-can-we-break-the-company-s-stranglehold and https://ilsr.org/amazon-stranglehold/; see also: http://www.nytimes.com/2016/12/13/opinion/forget-att-the-real-monopolies-are-google-and-facebook.html?_r=0 ; and: https://www.theguardian.com/commentisfree/2017/feb/19/the-observer-view-on-mark-zuckerberg , and https://www.theatlantic.com/technology/archive/2018/01/facebook-doesnt-care/551684/ .
For a survey indicating that users are concerned about this issue, see: https://ec.europa.eu/futurium/en/system/files/ged/ec_ngi_final_report_1.pdf .
For a very cogent historical analysis, making an analogy to the age of the Robber Barons, see: http://www.potaroo.net/ispcol/2017-03/gilding.html .
See also pp. 18-19 of the World Bank's 2016 Word Development Report (WDR-2016), titled "Digital Dividends", available at: http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf

[265] A forceful and well-reasoned call for regulation has been given by *The Economist*, see: http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource and

example, platforms might abusively use personal data to set high prices for goods for certain customers,[266] or a dominant national provider might impede the operation of an international competitor[267], or a dominant company may excessively influence governments[268], or a dominant search engine might provide search results that favor certain retail sites[269]. As the founders of Google put the matter back in 1998 (when they were graduate students): "we believe the issue of advertising causes enough mixed incentives that it is crucial to have a competitive search engine that is transparent and in the academic realm"[270].

95. Such corporate power can erode democracy, by in effect shifting power from the democratically elected representatives of the people to corporations, which not democratic entities. A scholarly article well documents the current trend towards shifing decision-making powers to privat companies and concludesr (the considerations below apply to many companies in addition to Amazon)[271]:

> Solutions to Amazon's power will, no doubt, be hard to advance as a political matter—consumers like 2-day deliveries. But understanding the bigger picture here is a first step. Political economy clarifies the stakes of Amazon's increasing power over commerce. We are not simply addressing dyadic transactions of individual consumers and merchants. Data access asymmetries will disadvantage each of them (and advantage Amazon as the middleman) for years to come. Nor can we consider that power imbalance in isolation from the way Amazon pits cities against one another. Mastery of political dynamics is just as important to the firm's success as any technical or business acumen. And only political organization can stop its functional sovereignties from further undermining the territorial governance at the heart of democracy.

https://www.economist.com/news/leaders/21735021-dominance-google-facebook-and-amazon-bad-consumers-and-competition-how-tame; see also: https://www.nytimes.com/2017/04/22/opinion/sunday/is-it-time-to-break-up-google.html ; and https://www.ip-watch.org/2017/05/09/republica-2017-strategy-empire-revealed-patents/ and pp. 52 ff. of http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf and https://www.insidetechmedia.com/2017/11/07/the-bundeskartellamt-publishes-a-paper-on-big-data-and-competition/ .

For a high-level outline of the issues, see Recommendation ITU-T D.261, Principles for market definition and identification of operators with significant market power – SMP.

[266] https://www.theguardian.com/technology/2017/jun/04/surge-pricing-comes-to-the-supermarket-dynamic-personal-data

[267] https://techcrunch.com/2016/11/28/ubers-china-app-is-now-separate-from-its-global-app-and-a-nightmare-for-foreigners/

[268] http://www.huffingtonpost.com/entry/google-monopoly-barry-lynn_us_59a738fde4b010ca289a1155?section=us_politics and https://www.nakedcapitalism.com/2017/08/new-america-foundation-head-anne-marie-slaughter-botches-laundering-googles-money.html

[269] The European Commission found that Google had done this, see:
http://europa.eu/rapid/press-release_STATEMENT-17-1806_en.htm
http://europa.eu/rapid/press-release_MEMO-17-1785_en.htm

[270] At the end of Appendix A of the paper by Brin and Page, "The Anatomy of a Large-Scale Hypertextual Web Search Engine" at http://infolab.stanford.edu/~backrub/google.html

[271] https://lpeblog.org/2017/12/06/from-territorial-to-functional-sovereignty-the-case-of-amazon/

96. As the Internet Society puts the matter on page 40 of its 2017 Global Internet Report: Paths to Our Future[272]: " … the scope of market change driven by dramatic advances in technology will inevitably force a fundamental rethink of existing approaches in competition law and traditional communications regulation. Data will increasingly be seen as an asset linked to competitive advantage, changing the nature of merger reviews, evaluations of dominance and, importantly, consumer protection."

97. Further, as already noted, control of large amounts of data may lead to dominant positions that impeded competition[273]. As a learned commentator puts the matter[274]:

> Five American firms – China's Baidu being the only significant foreign contender – have already extracted, processed and digested much of the world's data. This has given them advanced AI capabilities, helping to secure control over a crucial part of the global digital infrastructure. Immense power has been shifted to just one sector of society as a result.

98. Appropriate regulatory intervention might be different from that arising under present competition or anti-trust policies.[275] As one commentator puts the matter[276] (his text starts with a citation):

> "'*I do not divide monopolies in private hands into good monopolies and bad monopolies. There is no good monopoly in private hands. There can be no good monopoly in private hands until the Almighty sends us angels to preside over the monopoly. There may be a despot who is better than another despot, but there is no good despotism'*
> William Jennings Bryan, speech, 1899, quoted in Hofstadter (2008)
>
> The digital world is currently out of joint. A small number of tech companies are very large, dominant and growing. They have not just commercial influence, but an impact on our privacy, our freedom of expression, our security, and – as this study has shown – on our civic society. Even if they mean to have a positive and constructive societal impact – as they make clear they do – they are too big and have too great an influence to escape the attention of governments, democratic and non-democratic. Governments have already responded, and more will."

[272] https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf

[273] https://www.wired.com/story/ai-and-enormous-data-could-make-tech-giants-harder-to-topple/

[274] https://www.theguardian.com/commentisfree/2016/dec/04/data-populists-must-seize-information-for-benefit-of-all-evgeny-morozov

[275] https://www.competitionpolicyinternational.com/let-the-right-one-win-policy-lessons-from-the-new-economics-of-platforms/
https://www.washingtonpost.com/business/is-amazon-getting-too-big/2017/07/28/ff38b9ca-722e-11e7-9eac-d56bd5568db8_story.html .
An academic treatment of the topic is Khan, L. M. (2017) "Amazon's Antitrust Paradox", *The Yale Law Journal*, vol. 126, no. 3, pp. 564-907, available at: http://www.yalelawjournal.org/note/amazons-antitrust-paradox

[276] Martin Moore. *Tech Giants and Civic Power*. Centre for the Study of Media, Communication, and Power, King's College. April 2016. Available at: http://www.kcl.ac.uk/sspp/policy-institute/CMCP/Tech-Giants-and-Civic-Power.pdf

99. As a scholar puts the matter[277]:

> … the current framework in antitrust—specifically its pegging competition to "consumer welfare," defined as short-term price effects—is unequipped to capture the architecture of market power in the modern economy. … Specifically, current doctrine underappreciates the risk of predatory pricing and how integration across distinct business lines may prove anticompetitive. These concerns are heightened in the context of online platforms for two reasons. First, the economics of platform markets create incentives for a company to pursue growth over profits, a strategy that investors have rewarded. Under these conditions, predatory pricing becomes highly rational—even as existing doctrine treats it as irrational and therefore implausible. Second, because online platforms serve as critical intermediaries, integrating across business lines positions these platforms to control the essential infrastructure on which their rivals depend. This dual role also enables a platform to exploit information collected on companies using its services to undermine them as competitors.
>
> … [This paper] closes by considering two potential regimes for addressing [a dominant player's] power: restoring traditional antitrust and competition policy principles or applying common carrier obligations and duties.

100. As a well-researched report put the matter: "[Company X's] increasing dominance comes with high costs. It's eroding opportunity and fueling inequality, and it's concentrating power in ways that endanger competition, community life, and democracy. And yet these consequences have gone largely unnoticed thanks to [Company X's] remarkable invisibility and the way its tentacles have quietly extended their reach."[278]

101. As noted above, the dominance of certain platforms[279] raises issues related to freedom of speech, because some platforms apply strict rules of their own to censor certain types of content[280], and, for many users, there are no real alternatives to dominant platforms[281]; and some workers might also face limited choices due to dominant platforms[282].

[277] Khan, L. M. (2017) "Amazon's Antitrust Paradox", *The Yale Law Journal*, vol. 126, no. 3, pp. 564-907, available at: http://www.yalelawjournal.org/note/amazons-antitrust-paradox

[278] https://ilsr.org/amazon-stranglehold/

[279] For data regarding such dominance, see for example:
http://www.eecs.umich.edu/eecs/about/articles/2009/Observatory_Report.html
http://www.networkworld.com/article/2251851/lan-wan/the-internet-has-shifted-under-our-feet.html
http://www.xconomy.com/boston/2009/10/20/arbor-networks-reports-on-the-rise-of-the-internet-hyper-giants/
https://www.arbornetworks.com/blog/asert/the-battle-of-the-hyper-giants-part-i-2/

[280] See for example https://www.theguardian.com/technology/2016/sep/09/facebook-deletes-norway-pms-post-napalm-girl-post-row

[281] https://www.theguardian.com/technology/2016/nov/17/google-suspends-customer-accounts-for-reselling-pixel-phones

[282] https://www.nytimes.com/2017/03/21/magazine/platform-companies-are-becoming-more-powerful-but-what-exactly-do-they-want.html?_r=2

102. As *The Economist* puts the matter[283]:

> Prudent policymakers must reinvent antitrust for the digital age. That means being more alert to the long-term consequences of large firms acquiring promising startups. It means making it easier for consumers to move their data from one company to another, and preventing tech firms from unfairly privileging their own services on platforms they control (an area where the commission, in its pursuit of Google, deserves credit). And it means making sure that people have a choice of ways of authenticating their identity online.
>
> …
>
> … The world needs a healthy dose of competition to keep today's giants on their toes and to give those in their shadow a chance to grow."

103. As a well-known technologist reportedly stated in March 2017, the telecoms industry has evolved from a public peer-to-peer service – where people had the right to access telecommunications – to a pack of content delivery networks where the rules are written by a handful of content owners, ignoring any concept of national sovereignty.[284]

104. And, citing *The Economist* again[285]:

> The dearth of data markets will also make it more difficult to solve knotty policy problems. Three stand out: antitrust, privacy and social equality. The most pressing one, arguably, is antitrust …

105. As learned scholars have put the matter[286]:

> The question of how to make technology giants such as Google more publicly accountable is one of the most pressing political challenges we face today. The rapid diversification of these businesses from web-based services into all sorts of aspects of everyday life—energy, transport, healthcare—has found us unprepared. But it only emphasizes the need to act decisively.

106. An excellent overview of various methods that can be used to increase competition is provided in Wu, Tim, Antitrust Via Rulemaking: Competition Catalysts (October 24, 2017), *Colorado Technology Law Journal*.[287] Wu refers to actual examples (including in telecommunications) to show how regulations can be used to increase (or inadvertently fail to increase) completion. That is,

[283] http://www.economist.com/news/leaders/21707210-rise-corporate-colossus-threatens-both-competition-and-legitimacy-business

[284] https://disruptive.asia/transit-dead-content-literally-rules/

[285] http://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy

[286] In section 4.5 of Powles, J. and Hodson, H., Google DeepMind and health care in an age of algorithms, *Health and Technology*, 2017, pp. 1-17, Health Technol. (2017) doi:10.1007/s12553-017-0179-1, available at: http://link.springer.com/article/10.1007%2Fs12553-017-0179-1

[287] https://ssrn.com/abstract=3058114

regulatory intervention is means to be considered in parallel to, or instead of, judicial enforcement of antitrust/competition law.

107. Measures to ensure accountability may be needed with respect to labor-relation issues, and not only with respect to users and consumers.[288]

108. Large data sets are valuable only because they combine data from many individuals. Thus the value of the data is derived from the large number of people who contributed to the data. Consequently, "data is an essential, infrastructural good that should belong to all of us; it should not be claimed, owned, or managed by corporations."[289]

109. National authorities in a number of countries have undertaken investigations,[290] and even imposed measures,[291] in specific cases. And at least one influential member of a national parliament has expressed concern about some major Internet companies "because they control essential tech platforms that other, smaller companies depend upon for survival."[292] The Legal Affairs Committee of the European Parliament adopted an Opinion in May 2017 that, among other provisions[293]:

> Calls for an appropriate and proportionate regulatory framework that would guarantee responsibility, fairness, trust and transparency in platforms' processes in order to avoid discrimination and arbitrariness towards business partners, consumers, users and workers in relation to, inter alia, access to the service, appropriate and fair referencing, search results, or the functioning of relevant application programming interfaces, on the basis of interoperability and compliance principles applicable to platforms;

110. The topic is covered to some extent in paragraphs 24 ff. of a European Parliament Committee Report on online platforms and the digital single market, (2016/2276(INI).[294] And by some provisions in the national laws of at least one

[288] https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html?_r=2

[289] https://www.theguardian.com/commentisfree/2016/dec/04/data-populists-must-seize-information-for-benefit-of-all-evgeny-morozov

[290] See for example http://europa.eu/rapid/press-release_IP-16-1492_en.htm; http://europa.eu/rapid/press-release_IP-16-2532_en.htm and http://europa.eu/rapid/press-release_IP-15-5166_en.htm; a more general approach is described at: http://www.accc.gov.au/media-release/accc-to-undertake-market-study-of-the-communications-sector

[291] See for example http://www.autoritedelaconcurrence.fr/user/standard.php?id_rub=606&id_article=2534 and, in the case of Google: http://europa.eu/rapid/press-release_IP-17-1784_en.htm

[292] http://www.cnet.com/news/senator-warren-says-apple-google-and-amazon-have-too-much-power/

[293] http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-601.100&format=PDF&language=EN&secondRef=02

[294] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-599.814+01+DOC+PDF+V0//EN&language=EN

country.[295] Many of the issues relating to platforms and human rights have been well documented by the IGF Dynamic Coalition on Platform Responsibility.[296]

111. However, it does not appear that there is an adequate platform for exchanging national experiences regarding such matters.[297]

112. Further, dominant platforms (in particular those providing so-called "sharing economy" services) may raise issues regarding worker protection, and some jurisdictions have taken steps to address such issues.[298]

Recommendation 9.1

We recommend to invite UNCTAD to study the economic and market issues related to platform dominance[299], and to facilitate the exchange of information on national and regional experiences, and that the ILO be mandated to study the worker protection issues related to platform dominance and the so-called "sharing economy".

113. Further, dominant search platforms may, inadvertently or deliberately, influence election results, which may pose an issue for democracy.[300]

Recommendation 9.2

We recommend to invite the Inter-Parliamentary Union (IPU) and the UN HCHR to study the potential effects of platform dominance on elections and democracy.

[295] See section 3.2 of the following commentary on the French Digital Republic Law: https://www.lw.com/thoughtLeadership/French-digital-republic-law-english; see also the decrees issued in October 2017: http://proxy-pubminefi.diffusion.finances.gouv.fr/pub/document/18/22764.pdf

[296] http://bibliotecadigital.fgv.br/dspace/handle/10438/19402

[297] Except for certain specific issues relating to Over the Top (OTT) services and telecommunications operators which are discussed in ITU. A good summary of those specific issues is found in the section on OTT services of: http://www.itu.int/md/T13-WTSA.16-INF-0009/en

[298] See for example pp. 12 and 13 of http://library.fes.de/pdf-files/id-moe/12797-20160930.pdf and https://www.theguardian.com/technology/2016/oct/28/uber-uk-tribunal-self-employed-status and https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-05/cp170050en.pdf. A more general discussion of various issues arising out of platform dominance is at: http://www.alainet.org/en/articulo/181307

[299] We note in this context the existence in UNCTAD of the Intergovernmental Group of Experts on Competition Law and Policy, see: http://unctad.org/en/Pages/DITC/CompetitionLaw/Intergovernmental-Group-of-Experts-on-Competition-Law-and-Policy.aspx and the United Nations Set of Rules and Principles on Competition (TD/RBP/CONF/10/Rev.2), published in 2000 and available at: http://unctad.org/en/docs/tdrbpconf10r2.en.pdf

[300] https://newint.org/features/2016/07/01/can-search-engine-rankings-swing-elections/ and https://www.theguardian.com/world/2016/oct/27/angela-merkel-internet-search-engines-are-distorting-our-perception and http://singularityhub.com/2016/11/07/5-big-tech-trends-that-will-make-this-election-look-tame/ and http://money.cnn.com/2016/11/09/technology/filter-bubbles-facebook-election and http://www.pnas.org/content/112/33/E4512.full.pdf; and https://www.theguardian.com/technology/2016/dec/04/google-democracy-truth-internet-search-facebook for a possible impact on free speech, see: http://www.globalresearch.ca/google-corporate-press-launch-attack-on-alternative-media/5557677 .

10. How to deal with embedded software

114. More and more devices used in ordinary life, including in particular automobiles, depend more and more on software. Software is protected by copyright law. Thus users who buy a device have increasingly less control over the device, because they cannot change the software controls the device. This raises significant policy issues.[301] In fact, attempts to change the software may be criminal acts in some countries.

115. This situation may result in a significant shift of market power away from consumers, thus reducing competition. Indeed, a respected computer scientist has called for the establishment, at the national level of an "algorithm safety board"[302]. At present, there does not appear to be adequate consideration of these issues at the international level.

Recommendation 10

We recommend to invite UNCTAD and WIPO to study the issues related to embedded software, which include economic and legal issues.

11. Issues related to ccTLDs and gTLDs

116. The Tunis Agenda states:

> **68.** We recognize that all governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the Internet. **We also recognize** the need for development of public policy by governments in consultation with all stakeholders.
>
> **69.** We further recognize the need for enhanced cooperation in the future, to enable governments, on an equal footing, to carry out their roles and responsibilities, in international public policy issues pertaining to the Internet, but not in the day-to-day technical and operational matters, that do not impact on international public policy issues.

117. As noted above, issues related to ccTLDs and gTLD are squarely within the mandate of enhanced cooperation. Policies relating to ccTLDs and gTLDs are developed and maintained by the Internet Corporation for Assigned Names and Numbers.

11.1 Equal treatment for ccTLDs

118. On 6 June 2016, as part of the IANA transition process, the Internet Corporation for Assigned Names and Numbers (ICANN) and the US National

[301] http://copyright.gov/policy/software/

[302] http://www.techworld.com/big-data/pioneering-computer-scientist-calls-for-national-algorithms-safety-board-3659664/; see also https://www.technologyreview.com/s/608248/biased-algorithms-are-everywhere-and-no-one-seems-to-care/ and https://www.technologyreview.com/s/607955/inspecting-algorithms-for-bias/

Telecommunications and Information Administration (NTIA) exchanged letters[303]. In its letter, ICANN confirmed that it will not take any action to re-delegate the top-level domain names ".edu", ".gov", ".mil", and ".us" (which are administered by the US Government) without first obtaining express written approval from NTIA.

119. This exchange of letters is presumably a binding contract between ICANN and the US government. That is, ICANN cannot take actions regarding these domain names without the agreement of the US government.

120. The top-level domain name ".us" is a country code domain name, that is, a ccTLD.

121. According to the Principles and Guidelines for the Delegation and Administration of Country Code Top Level Domains[304] of ICANN's Government Advisory Committee (GAC), approved on 5 April 2005 (emphasis added):
"4.1.2. Every country or distinct economy with a government or public authority recognised in accordance with article 3.8 above should be able to ask for its appropriate country code to be represented as a ccTLD in the DNS and to designate the Registry for the ccTLD concerned."

122. The term "should" is used elsewhere in the cited GAC Principles and Guidelines.

123. Thus the cited GAC Principles and Guidelines do not create a binding obligation for ICANN not to take actions regarding ccTLDs without the agreement of the concerned government.

124. In line with the principles of equal footing and equal roles and responsibilities of all governments enunciated in the Tunis Agenda, all government should be treated equally with respect to their ccTLD.

125. Consequently, we propose the following recommendation.

[303] https://www.ntia.doc.gov/page/exchange-letters-us-government-administered-tlds

[304] https://gacweb.icann.org/display/GACADV/ccTLDs?preview=/28278844/28475457/ccTLD_Principles_0.pdf

Recommendation 11.1

In order to further implement enhanced cooperation, we recommend to invite ICANN to provide to all governments equal treatment with respect to their ccTLDs.
Specifically, it is proposed to invite ICANN to agree to exchange letters with any country that so requests, stating that it will not take any action to re-delegate the country's ccTLD without first obtaining express written approval from the government of the country in question.
And it is proposed to invite ICANN to delegate to any country that so requests up to three additional ccTLDs, with names of the form "ccXYZ", where "cc" is the two-letter country code, and "XYZ" are strings chosen by the country, for example "gov", "mil", "edu", or "01", "02", "03". Thus, if "rt" were a valid country code (which it is not), the corresponding country could request delegation of "rtgov" or "rt01" etc.

11.2 Agreements regarding jurisdiction

126. In the process of revising its bylaws as part of the IANA transition process, the Internet Corporation for Assigned Names and Numbers (ICANN) has explicitly chosen to subject itself to the laws of California, see for example articles 6.1(a) and 24.1 of the new bylaws[305]. Further, ICANN's articles of incorporation[306] specify that it is a California corporation. Article 6 of the bylaws and the articles of incorporation can only by changed upon approval by a three-fourths vote of all the Directors and the approval of the Empowered Community[307]. A change to a fundamental bylaw is approved by the Empowered Community only if it is not objected to by more than one member of that body[308].

127. Since ICANN is legally a US entity, it is subject to the jurisdiction of US courts[309]. US courts have exercised that jurisdiction in the past[310].

[305] https://www.icann.org/en/system/files/files/adopted-bylaws-27may16-en.pdf

[306] https://www.icann.org/resources/pages/governance/articles-en

[307] See article 25 and 25.2(b).

[308] See 1.4(b)(ii) of the Annex D of the bylaws.

[309] A detailed explanation of why this is significant, including the historical background of the issue, is provided at:
http://cis-india.org/internet-governance/blog/jurisdiction-the-taboo-topic-at-icann ; a shorter account is provided at:
http://www.epw.in/journal/2016/42/web-exclusives/internet-governance.html ; see also:
http://www.internetgovernance.org/2017/07/20/icann-and-jurisdiction-working-group-reaches-critical-juncture/

[310] See for example https://www.icann.org/news/announcement-2-2016-03-05-en and
https://www.prlog.org/12539064-united-states-court-has-granted-an-interim-relief-for-dca-trust-on-africa.html
and the court case filed just prior to the IANA transition:
https://www.texasattorneygeneral.gov/files/epress/Net_Complaint_-_FILED.pdf
http://ia601506.us.archive.org/17/items/gov.uscourts.txsd.1386946/gov.uscourts.txsd.1386946.7.0.pdf
http://ia601506.us.archive.org/17/items/gov.uscourts.txsd.1386946/gov.uscourts.txsd.1386946.10.1.pdf

A full compendium of litigation concerning ICANN is found at:
https://www.icann.org/resources/pages/governance/litigation-en

128. In line with the principles of equal footing and equal roles and responsibilities of all governments enunciated in the Tunis Agenda, ICANN should not be subject to the jurisdiction of a particular country.

129. One solution would be for the USA (or some other country) to grant some form of immunity to ICANN.

130. But, since ICANN has chosen to subject itself to the jurisdiction of the USA, it does not appear that ICANN would accept some form of immunity. And indeed discussions within ICANN regarding that matter did not result in consensus[311], so it appears unlikely that any such immunity would be requested, much less granted.

131. Therefore it seems more appropriate to recommend what follows in order to avoid a court ordering ICANN to re-delegate a ccTLD or to reassign IP addresses[312].

Recommendation 11.2

We recommend to invite concerned states to make a binding agreement with each other to the effect that they would not exercise their jurisdiction over ICANN in ways that would violate the principles of equal footing and equal roles and responsibilities of all governments.

132. Such a binding agreement would have to take the form of a treaty. The exact language of the treaty would have to be carefully negotiated. Therefore we also propose the following.

Recommendation 11.3

We recommend to invite concerned states to consider the matter of agreeing to refrain to exercise jurisdiction over ICANN in certain ways and to convene a treaty negotiation on this matter.

133. Further, the IANA transition process provides that the management and operation of the authoritative root zone server will continue to be provided by Verisign, but under a contract with ICANN, and not under a contract with the US government as was the case in the past.[313]

134. This decision was not the result of a public consultation. Verisign is a US company, subject to US jurisdiction, so US courts could order Verisign directly to change the root, they don't necessarily need to order ICANN to do so. So long as Verisign had a contract with the US government, it was unlikely that Verisign

[311] See http://mm.icann.org/pipermail/ws2-jurisdiction/2017-October/001888.html and http://mm.icann.org/pipermail/ws2-jurisdiction/2017-October/001896.html

[312] This example is not theoretical. The equivalent of such remedies, namely "attachment" has been requested in a lawsuit involving Iran, see: https://www.icann.org/resources/pages/icann-various-2014-07-30-en
and in particular page 1 of https://www.icann.org/en/system/files/files/appellants-brief-26aug15-en.pdf

[313] https://www.icann.org/news/blog/root-zone-management-transition-update-preservation-of-security-stability-and-resiliency

could be sued directly, because it was just implementing whatever NTIA told it do. But now the US government is no longer in the loop, so Verisign can be sued directly.

135. Further, ten of the thirteen root servers which provide the data used by all other instances of root servers are managed by US entities (three of which are US government agencies: NASA, Defense Systems Information Agency, and US Army); the other three servers are managed by entities in Japan, the Netherlands, and Sweden.[314] An operator of a root server could misuse it in various ways, in particular to collect certain types of data or to degrade certain services.[315]

136. We propose the following recommendation to address these matters.

Recommendation 11.4

We recommend to invite all concerned states to enter into a binding agreement to the effect that they will not exercise their jurisdiction over any root zone server, or over the operator of the authoritative root zone file, in ways that would violate the principles of equal footing and equal roles and responsibilities of all governments.

11.3 Protection of country names in the DNS

137. In 2000, the World Intellectual Property Organization was requested by 20 states to study certain intellectual property issues relating to Internet domain names that had not been considered in the First WIPO Internet Domain Name Process, including protection of geographic identifiers.[316]

138. WIPO duly studied the issues and, on 21 February 2003, informed ICANN[317] that its Member States formally recommended, inter alia, that country names should be protected against abusive registration as domain names. The decision to make that recommendation was supported by all Member States of WIPO, with the exception of Australia, Canada and the United States of America, which dissociated themselves from the decision. Japan also expressed certain reservations. WIPO recommended that the protection of country names should be implemented through an amendment of the Uniform Dispute Resolution Policy (UDRP) and should apply to all future registrations of domain names in the gTLDs.

139. The recommendation was discussed in ICANN, but it was not agreed and, consequently, the UDRP was not modified. Thus, at present, the UDRP does not protect country names.

140. Following the privatization of ICANN on 1 November 2016, this matter was brought to the attention of the ITU World Telecommunication

[314] See https://en.wikipedia.org/wiki/Root_name_server
[315] See http://www.cavebear.com/old_cbblog/000232.html
[316] http://www.wipo.int/amc/en/processes/process2/index.html
[317] http://www.wipo.int/export/sites/www/amc/en/docs/wipo.doc

Standardization Assembly (WTSA) in Addendum 22 to Document 42-E[318], which states:

> There are two main categories of Top Level Domains, Country Code (ccTLDs) and Generic (gTLDs). One of the differences between the administration of the ccTLDs and the gTLDs is the national sovereignty of the administration of the ccTLDs as opposed to the global and ICANN managed administration of gTLDs.
>
> While WTSA focuses on ccTLDs, the recent expansion of generic TLDs initiated in 2012 by ICANN introduced many new applications some that have geographic implications, which require addressing various challenges, including resolution of various conflicts. **Therefore "*special attention should be given to the issue of geographic gTLDs as a concept (in generic terms), as they intersect with core areas of interests of any state*"**.

141. The submission to WTSA provides a summary of events relating to the delegation of the gTLD ".africa" and states:

> These challenges to delegating a regional geographic Top Level Domain raises important principle concerns for the Africa region and others over the issue of jurisdiction, who should control the delegation of critical regional geographic names like dot Africa, the role of governments and intergovernmental organizations in the ICANN multi-stakeholder model and the effectiveness and reliability of government protection mechanisms for ccTLDs and geographic names related to their distinct regions.

142. The submission to WTSA proposed, inter alia, to instruct ITU-T Study Group 2:

> 2 to study necessary measures that should be taken to ensure that country, territory and regional names must be protected and reserved from registration as new gTLDs; and that these names should include but not be limited to capital cities, cities, sub-national place names (county, province or state) and geographical indications;
>
> 3 to study, in collaboration with relevant bodies, on ways and means to maintain the right of Member States to request the reservation and to oppose the delegation of any top-level domain (even if it is not included on that list) on the basis of its sensitivity to regional and national interests,

143. The matter was discussed at WTSA, but no agreement was reached on whether ITU-T should study the matter, and if so how[319]. Consequently, the following recommendation is proposed.

[318] http://www.itu.int/md/T13-WTSA.16-C-0042/en

[319] See DT/60, http://www.itu.int/md/T13-WTSA.16-161025-TD-GEN-0060/en

Recommendation 11.5

We recommend to invite all concerned countries to transpose into their national law the WIPO recommendations of 21 February 2003 regarding the protection of country names against abusive registration as domain names, so that they could be enforced in all countries that have jurisdiction over ICANN.

11.4 OFAC licenses

Recommendation 11.6

We recommend to facilitate participation by individuals and/or entities from certain countries in ICANN matters[320] by inviting ICANN to consider taking the following actions:

1. Request a general OFAC waiver from the U.S. Commerce Department

2. Contractually oblige registrars to investigate the possibility of receiving an OFAC license for providing services to sanctioned countries

3. Prohibit registrars from arbitrarily cancelling domain names without notice

4. Obtain a legal opinion regarding whether registrars based in other countries need to comply with OFAC and US laws in general

5. Take any other actions which may alleviate the problem

12. Roles and Responsibilities

Recommendation 12

We recommend to invite all stakeholders to consider revisiting the roles and responsibilities of the several stakeholders outlined in paragraph 35 of the Tunis Agenda in light of developments and discussions that have taken place over the past 10 years. Specifically, we recommend considering the following revisions to paragraph 35 of the Tunis agenda:

> **35. We reaffirm** that the management of the Internet encompasses both technical and public policy issues, which may be inter-related, and should involve all stakeholders and relevant intergovernmental and international organizations. Decisions should always be informed as appropriate by inputs from stakeholders. In this respect it is recognized that:

[320] For the background, see: http://www.internetgovernance.org/2017/01/13/icanns-jurisdiction-sanctions-and-domain-names/ and http://www.internetgovernance.org/2017/07/20/icann-and-jurisdiction-working-group-reaches-critical-juncture/

a) Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for ~~international~~ Internet-related public policy issues, and in particular for the protection of all human rights. Decisions should be informed by inputs from other stakeholders as appropriate.
b) The private sector has had, and should continue to have, an important role in the development of the Internet, both in the technical and economic fields, and in providing objective factual information to policy decision-makers, so as to further the public interest and to achieve the shared goal of an equitable information society.
c) Civil society has also played an important role on Internet matters, ~~especially at community level~~ at both the national and international levels, and should continue to play such a role. Further, it should provide views, opinions, and information to policy decision-makers and should be invited to comment, as appropriate, regarding public policy issues at both the national and international levels. Representatives, if representation is needed, should be selected through open, democratic, and transparent processes. Internal processes should be based on inclusive, publicly known, well defined and accountable mechanisms.
d) Intergovernmental organizations have had, and should continue to have, a facilitating role in the coordination of Internet-related public policy issues and in the harmonization of national laws and practices.
e) International organizations have also had and should continue to have an important role in the development of Internet-related technical standards and relevant policies.

The respective roles and responsibilities of stakeholders should be interpreted in a flexible manner with reference to the issue under discussion.

5 April 2018

Association of School and College Leaders (ASCL) and Self-Esteem Team (SET) – written evidence (IRN0005)

1. The Association of School and College Leaders (ASCL) represents over 19,000 education system leaders, heads, principals, deputies, vice-principals, assistant heads, business managers and other senior staff of state-funded and independent schools and colleges throughout the UK. ASCL members are responsible for the education of more than four million young people in more than 90 per cent of the secondary and tertiary phases, and in an increasing proportion of the primary phase. This places the association in a strong position to consider this issue from the viewpoint of the leaders of schools and colleges of all types.

2. The Self-Esteem Team (SET) was founded in 2013 by Nadia Mendoza and Grace Barrett and over the last five years they have toured the UK's schools and worked with tens of thousands of young people, to help equip them with tools to navigate their mental health, manage the relationship with their bodies, and build self-esteem including how they behave and relate to social media.

3. ASCL and SET have jointly considered the impact of social media use by children and young people, children and young people's safety and mental health and regulation of the internet, particularly social media.

4. This hugely relevant issue is of crucial importance to us from both a school leader's and a young person's point of view. Both organisations welcome this inquiry in respect of regulating the internet for use by children and young people because we believe that for many children and young people this is an important issue that needs urgent attention.

5. School and college leaders and young people agree that social media can be a force for good but acknowledge that it also has a dark side. While it can help young people (and adults) connect with others in a positive way it is a technology which has grown at great speed without educators, parents, policy makers or indeed children and young people themselves understanding what the implications may be for their relationships, safety and mental health and wellbeing or how their data may be used now or in the future.

6. The recent stories about Facebook data harvesting call into focus huge questions about personal information and privacy and stories such as the Toby Young saga over his appointment to the Board of the Office for Students show clearly what one may have said on social media in the past could impact on a person's future chances and opportunities. Children and young people have grown up with social media but there is no clarity as to how this information could impact on them in the future.

7. We believe that as a society there needs to be a much greater understanding of how social media can impact on us all and particularly on children and young people and we need clear strategies for how to mitigate against the negative impacts. These effects can be around wellbeing, mental health and self-esteem as well child protection and safeguarding and privacy now and in the long term.

8. ASCL members and young people themselves want government and the technology companies to do more to protect young people and to help them to develop healthy relationships on and offline so that they can enjoy social media safely and responsibly.

9. The Association of School and College Leaders (ASCL) surveyed 460 secondary school headteachers in England, Wales and Northern Ireland in January 2018. These headteachers lead a wide range of schools in both the state and independent sectors[321]. They were asked about the impact on pupils of social media use over the past 12 months. The results are stark and unequivocal:

- 95% felt that the mental health and wellbeing of a proportion of their pupils had suffered as a result of social media use.

- 39% said more than half of their pupils were affected. 460 responded to the question 'Do you think the mental health and wellbeing of pupils has suffered as a result of social media use over the past 12 months?'
  No pupils affected 0.00% 0
  1% to 10% of pupils affected 5.87% 27
  11% to 25% of pupils affected 20.87% 96
  26% to 50% of pupils affected 29.57% 136
  51% to 75% of pupils affected 21.52% 99
  75% to 90% of pupils affected 12.17% 56
  More than 90% of pupils affected 5.00% 23
  Don't know 5.00% 23

- Almost all (459/460) had received reports of pupils being bullied on social media and 40% said incidents were reported on a daily or weekly basis.

- Almost all (457/460) had received reports of pupils encountering upsetting material on social media – such as sexual content, self-harm, bullying, or hate speech, with 27% saying such incidents were reported on a daily or weekly basis.

[321] In January 2018 ASCL carried out an online survey circulated by email to the headteachers of secondary schools in England, Northern Ireland and Wales in. It was completed by 460 respondents. Most respondents (420) are from schools in England, with 25 from Wales, and 15 from Northern Ireland. They are from a wide range of schools including academies (48%), maintained schools (23%), independent schools (11%) and grammars (7%). For more information please contact richard.bettsworth@ascl.org.uk

- 89% had received reports of pupils being approached by strangers on social media sites.

- 93% had received reports of pupils experiencing low self-esteem as a result of seeing idealised images and experiences on social media, with 22% saying that pupils reported such feelings on a daily or weekly basis.

- 96% had received reports of pupils missing out on sleep as a result of social media use, with 32% saying they received such reports on a daily or weekly basis.

- 93% said that new laws and regulation should be introduced to ensure social media sites keep children safe

- 77% said the government and social media companies should produce more information for parents.

10. In the survey, headteachers described a wide range of activities in their schools to teach children to stay safe and well online. These include personal, social, health and economic (PSHE) and IT lessons, discussion sessions, speakers and seminars, assemblies, and dedicated awareness days.

11. Headteachers said social media misuse occurs outside of school but the problems it causes then spill over into school time and distract young people from learning.

12. Many felt that parents should take more responsibility and needed more information about how to keep their children safe online.

13. Headteachers also reported how social media misuse led to severe welfare issues, such as young people self-harming.

14. Individual headteacher comments:
    - “Whilst the school educates students and imposes limits of acceptable use, many parents are unable or unwilling to apply limits at home. A very small number of parents also behave badly on social media. When the school arranges e-safety meetings for parents there is very limited attendance. A national campaign to educate parents and alert them to the dangers of social media would support the education that is happening in schools for students.”

    - “Far too frequently parents join in with trolling or abuse incidents or model abusive or harmful social media behaviour to their children themselves; the classic example being parents wading in on social media with threats of violence or confrontation to 'protect' their own child.”

- "The number of issues the school is having to resolve weekly and sometimes daily as a result of bullying through social media that occurs outside of school, has increased rapidly and substantially. Not only does this have a detrimental effect on the well-being of individual pupils, but it also is having an impact on learning and progress and is diverting valuable and scarce resources away from the classroom."

- "We regularly have to deal with peer conflict, which often extends amongst families and the wider community and which has started on social media out of school hours. This not only takes up valuable resources, but also detracts from our main purpose of educating young people."

- "Pupils' use of social media has accelerated in the past five years and at the same time, reporting of mental health issues, self-harming and threatened suicide have increased. Five years ago our safeguarding log had one entry per week at most - now it is daily."

- "We have seen a big increase in cases of self-harm related to the use of social media. When in the past the first weeks after a break used to be quiet they are now much worse as pupils seek to settle arguments that have been enhanced over the holidays."

15. In March 2018 SET put out a call on social media to garner thoughts from young people about what they love and loathe about social media. Some of the responses both positive and negative are reproduced below:

    - 'I actually have friends now! Proper actual ones whose birthday parties I go to who come to stay and it's nice.'

    - 'It was Tumblr blogs that got me through the hell that was 'coming out'. I had no LGBTQ+ education or community except for online.'

    - 'I found amazing opportunities through social media.'

    - 'I use twitter/blogs for screaming into the void.'

    - 'I have so many support networks I couldn't get through without. Especially in the absence of professional help.'

    - 'There should be more info on block and mute functions. Social media was used by people I knew to tell me to injure or kill myself for being gay and there was nothing anyone could do either to support me or to deal with it. It's also easy to find pro self-harm/ana/mia sites when searching for help.'

    - 'I always wanted more info on how social media and marketing interact.'

- ‘It is good for creative inspiration and feeling connected with the world but it can make you feel lonely or insufficient. It's also good to pass time when you feel like doing nothing but can be a distraction at other times.’

- ‘Positive =uplifting pages like this one negative=there are loads it's awkward I believe because this depends on what you allow and keep around starting with "friends" "mum friends " that are actually putting you more down and just being generally fake with no real "support" for you in mind to my surprise I've had more support from total strangers than people in my friends list and to realise that I was actually used to those bullies coz they wore a mask called friend or family’

- I think that social media platforms need more moderators online to remove comments, picture... that could be seen as offensive or hurtful to someone else.

- Definitely agree with previous comments about community and finding like-minded people. On the flip side, it can make you feel more alone; if you compare yourself to others/don't belong to an online 'group' you can feel left out. In a social/school setting more, so young people are thinking about it more consciously instead of being subject to the subconscious thoughts it gives

16. In October, the government launched a strategy to make Britain “the safest place in the world to be online” with proposals for a voluntary code of practice for social media providers.

17. You can see from the ASCL survey that headteachers are not convinced that a voluntary code will be sufficient with 93% saying that new laws and regulation should be introduced to ensure social media sites keep children safe. We believe that such a code is needed and it should be mandatory backed up by an independent regulator.

18. In the autumn 2017 crossbencher Baroness Beeban Kidron put forward an amendment to the Data Protection Bill calling for technology companies to be subject to “minimum standards of age-appropriate design”. Her amendments won the support of senior politicians across the political spectrum as well as respected children’s organisations including NSPCC, Parent Zone, YoungMinds, the Anti-Bullying Alliance, Child Health Information Services and the Children’s Commissioner.

19. The proposed amendments which would have required the Information Commissioner to create guidance after consultation which could include:
    - high privacy settings by default for child users
    - not revealing their GPS location and minimal use of their data
    - not sending notifications during school hours or sleep hours
    - deactivating features designed to promote extended use
    - making sure commercially driven content is visible to and understood by a minor

- reporting processes with an end-point and a reasonable expectation of resolution

20. Proposals such as those listed above look very sensible to us. They were withdrawn with a promise from government to further develop its internet safety strategy with the government minister Lord Ashton of Hyde referring to the governments Internet Safety Strategy Green Paper consultation and we are aware that government is currently analysing the feedback to this. We consider that a voluntary duty on the technology industry will not be enough.

21. While we recognise that the government is trying to find solutions we are not convinced that the current proposals go far enough. We would like to explore the options for more stringent safeguards and more public information for parents.

22. **Answers to your questions (note we have not answered all Qs as we do not have the expertise to do so).**

Q1 Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

For the reasons stated in this response we believe that it is necessary to introduce specific regulation for child users of the internet particularly on social media platforms and any platform where they are able to connect with other people.

Q3 *How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?*

We do not believe that online platforms are moderating content in a sufficiently rigorous way as evidenced both by what school leaders and children say as outlined above. We supported Baroness Beeban Kidron’s amendment described above which would have had the Information Commissioner create guidance after consultation but we are not experts on how this should be done.

Q4 What role should users play in establishing and maintaining online community standards for content and behaviour?

In the case of children and young people we think that self-moderation must only be part of the picture.

23. ASCL has also responded to the government consultation on Changes to the teaching of Sex and Relationship Education and Personal, Social and

Health Education[322] ASCL members agree that schools should be teaching pupils about internet safety including the risks of accessing online pornography as well as teaching them what they need to know to be safe online, beyond what is already in the computing curriculum. But schools and colleges cannot do this work in a vacuum. ASCL has also responded to Transforming children and young people's mental health provision: a green paper[323].

24. We do not have all the answers but we believe that a debate about the impact of social media on children and young people and the lack of its regulation that includes the views of children and young people is much needed. The evidence from our members and young people themselves clearly indicates that we should not carry on as we are.

25. I hope that this is of value to your consultation, ASCL and SET are willing to be further consulted and to assist in any way that it can.

27 April 2018

[322] The ASCL response can be found here; https://www.ascl.org.uk/utilities/document-summary.html?id=40F4CE91-B129-4BAB-8B3843BD40C7EE88

[323] The ASCL response can be found here; https://www.ascl.org.uk/policy/consultation-responses_news-detail.transforming-children-and-young-people-s-mental-health-provision-a-green-paper.html

Dr Shehar Bano - written evidence (IRN0114)

About the author.

I received my Ph.D. (Computer Science) degree from University of Cambridge in 2017, after which I joined University College London as a postdoctoral researcher in the Information Security Research Group. I am an expert on the security and measurement of networked systems. My research illuminates the technical feasibility and consequences of information control by governments as well as online platforms. I have studied state-level censorship in Pakistan and China, and developed comprehensive models that capture its components and actors, their relationships and dependencies, and the underlying economics. In the context of online platforms, my research revealed a new kind of information control---*differential treatment*---where websites reject or restrict information access of certain classes of users. In collaboration with BuzzFeed, I studied the ecosystem of websites that serve hyperpartisan political news. Currently, in collaboration with Chainspace (a company I co-founded based on my research on scalable, privacy-preserving smart contract platforms), I am investigating how decentralised systems, such as those based on blockchains, can enable transparency.

This submission is the synthesis of my personal views on Internet regulation. I focus on the technical feasibility of state-level censorship, and information control by online platforms.

Technical feasibility of state-level censorship.

It is useful to consider that the Internet is comprised of a number of stakeholders including: (1) those who support the infrastructure that physically or logistically enables online communications (e.g., Internet Service Providers and Domain Name Registrars); (2) those who facilitate the publication or exchange of information (e.g., Facebook and Telegram); (3) those who provide services to support (e.g., Content Delivery Networks), optimise (e.g., Google Search), or monetise (e.g., Ad networks) the former; and (3) consumers of information (i.e., users).

Many governments around the world enforce Internet regulation via censorship, i.e. by requiring installation of filters at the national communication choke points such as Internet Service Providers (ISPs) and Internet Exchange Points (IXPs). State-level censorship is not technically feasible because of two reasons:

(1) It is not feasible to accurately identify the targets of regulation because the Internet is highly dynamic: information is served from different IP addresses over time; and the information itself is usually dynamically generated (e.g., based on time, and users' geographic location and other characteristics).

(2) The Internet is a complex ecosystem comprised of a number of potentially interdependent stakeholders (as discussed earlier): regulating one stakeholder can create a ripple effect, leading to unintended consequences on a range of other stakeholders (called 'False Positives').

I empirically showed the above limitations in my study[324] of Pakistan's regulation of online adult and video streaming content (YouTube) between 2011--2013. The first case highlighted limitations in comprehensively enumerating websites that fall under a certain category, in this case adult content. A number of websites were misclassified as adult websites and wrongly blocked. Moreover, a large fraction of users continued to successfully access adult websites that were not included in the government's censorship blacklist. These websites were either those that the blacklist failed to capture, or the old blocked websites resurfaced under new identities (IP address, domain name).

The second case, i.e. the YouTube block, highlighted the indirect costs incurred by Internet Service Providers due to 'unnatural' patterns emerging in users' browsing habits due to censorship. The YouTube block spurred a large fraction of users to employ mechanisms to get around the censorship by relaying their Internet traffic via servers located outside the country. As a result, the Internet Service Provider's local traffic optimisation techniques were undermined, forcing it to purchase additional bandwidth.

Though this study was conducted in a specific context, the technical limitations of Internet regulation that it highlights are broadly relevant. The effect of these challenges on legislation is that it will frequently miss the intended targets, and flag wrong targets potentially affecting other unintended targets too (collateral damage). A study by researchers at the University of Cambridge investigated the effectiveness of website takedowns, i.e. forcing ISPs and domain name registrars to remove websites. They found that there can be errors as well as intentional misuse in the process due to taking down legitimate websites which are "eventually returned to the registrants after being taken down by law enforcement, but after much time and many legal challenges".[325] Other studies note that the collateral damage of state-level censorship extends internationally to Internet users outside the censored country.[326, 327]

Technical feasibility of moderating the content that online platforms host.

In the traditional publication model, content-creators send their publication draft to a publisher, who gets an editor to check the draft for quality and publishing policy compliance, and then publishes it following the editor's approval. This whole process takes days (or weeks)---and only attracts somewhat motivated content-creators who are willing to undergo the editorial process, and do not mind the wait.

[324] "A Look at the Consequences of Internet Censorship Through an ISP Lens". Shehar Bano, Mobin Javed, Syed Ali Khayam, Zartash Afzal Uzmi and Vern Paxson. ACM SIGCOMM conference on Internet measurement (IMC), 2014.

[325] "Taking Down Websites to Prevent Crime". Alice Hutchings, Richard Clayton and Ross Anderson. APWG Symposium on Electronic Crime Research (eCrime) 2016.

[326] "The Collateral Damage of Internet Censorship by DNS Injection". Anonymous. SIGCOMM Computer Communications Review, 42(3):21–27, June 2012.

[327] "Routing Gone Wild: Documenting Upstream Filtering in Oman via India". Technical report, Citizen Lab. July 2012.

In my response below, I focus on online platforms that have turned this model around, by allowing users to publish their content nearly instantaneously, at the touch of their fingers. Online platforms have achieved this by delegating the editorial responsibilities to users (who essentially become both content-creators and editors)---their stance is that they only serve as a platform or a gateway that hosts this content, but does not accept any liability for it.

Online platforms do have acceptable usage and content moderation policies, but these are usually enforced (by removing content or penalising users) post facto, in response to user complaints. The alternative model is preemptive content moderation, where online platforms remove (or filter) objectionable content before publication. However, preemptive moderation of high volume user-generated content is extremely challenging. I describe below the technical challenges, which is my area of expertise, and do not comment on the social, ethical, and jurisdictional challenges.

Online platforms are tasked with having to moderate an enormous volume of a constant stream of user-generated content. The task can be automated to a degree, but human judgement is still necessary because of two reasons. First, automated detection may reflect biases from the data on which it is trained,[328] for example for only some kind of hate speech but not others. These systems could also be deliberately 'gamed', for example by reporting non-abusive posts, or using obscure words. Second, automated tools are not good at discerning contextual nuances (e.g., when should nudity be perceived as art v/s obscenity?), and to identify a suitable level of intervention (ignore, display warning to viewers, remove, report to the police etc.). Therefore, some of these platforms have recruited human moderators. This might be effective for small to medium platforms---but large platforms just cannot scale to the magnitude and velocity of data produced by billions of their users.

Legal liability and the challenge of attribution.

A challenge in deciding whether platforms should be held legally liable for the content they host is due to difficulty in attribution. So far we only considered the simple case where online platforms host only their own content. However, most platforms also embed content from third parties in real time, e.g., online advertising, product reviews and user comments. Some platforms go a step further, and merely aggregate / showcase content from third-party websites. Should these platforms be liable for oversights of the third parties? Facebook received wide criticism following the revelation of Russian interference in the 2016 US election via Facebook ads. But if those ads were pulled from a third party, would we blame Facebook or the third party (which itself may have used the services of another third party, and so on)? What makes it even more complex, for auditing purposes, is that it might not be possible to reproduce the interactions that led to certain content appear on a platform. A recent study[329]

[328] “Semantics Derived Automatically from Language Corpora Contain Human-like Biases”. A Caliskan, J Bryson, A Narayanan. Science 356 (6334), 183-186.

[329] “Discrimination in Online Advertising: A Multidisciplinary Inquiry”. Amit Datta, Anupam Datta, Jael Makagon, Deirdre K. Mulligan, and Michael Carl Tschantz. Conference on Fairness, Accountability and Transparency, 2018.

highlights similar challenges in the legal analysis of a real case which found gender-based discrimination in employment-related advertisements.

Transparency and fairness in content hosted by online platforms.

Online platforms can control both *what* information is presented to their users (the content), as well as *how* it is presented (the format). The human brain has limited capacity for processing information and the time span for which their interest is sustained; therefore the order and format in which information is presented to users is crucial (e.g., Google search engine ranking, or the posts that appear at the top of a user's Facebook timeline). Online platforms use opaque algorithms to decide the content and format of information that is presented to users. Some of these algorithms---from online advertisement, through online recommenders, to predictive policing---are biased, and at times outright discriminatory.[330]

Online platforms also have the responsibility to fairly offer their services to users, without any discrimination. I found empirical evidence of such discrimination in my study[331] of how users of anonymity software Tor experience the Web. Tor enables users to privately browse the Internet, without being censored by authoritarian governments. For millions of users around the globe, Tor is the only means to freely express themselves and get their voice heard. My study revealed that a significant number of websites treat Tor users differently than other users, either via outright rejection or by subjecting them to a degraded service. In another study,[332] I found that users of ad blocking software receive similar treatment. Both Tor and ad blocking software enhance user privacy, and by subjecting their users to such differential treatment, online platforms are effectively coercing those users to give up their privacy protections. In the first case, I found that online platforms inherited the differential treatment policies of their web hosting providers. This example reiterates the challenges in attribution stated previously.

The impact of the dominance of a small number of online platforms.

Over time the Internet has evolved into an ecosystem dominated and controlled by a small number of large online platforms---resulting in centralisation and monopolies.[333] In some ways this is good, for example by providing users with a convenient way to publish and discover content without bothering about the intricate technical details. But the ability of a few large players to influence information flows of billions of users over the Internet threatens users' right to free and fair access to information.

[330] https://fatconference.org/2018/program.html

[331] "Do You See What I See? Differential Treatment of Anonymous Users". Shehar Bano, David Fifield, Sadia Afroz,Mobin Javed, Srikanth Sundaresan, Vern Paxson, Steven J. Murdoch, and Damon McCoy. The Network and Distributed System Security Symposium (NDSS), 2016.

[332] "Ad-Blocking and Counter Blocking: A Slice of the Arms Race". Rishab Nithyanand, Shehar Bano, Mobin Javed, Narseo Vallina-Rodriguez, Marjan Falahrastegar, Julia E. Powles, Emiliano De Cristofaro, Hamed Haddadi and Steven J. Murdoch. The USENIX Workshop on Free and Open Communications on the Internet (FOCI), 2016.

[333] "The Barriers to Overthrowing Internet Feudalism". Tai Liu, Zain Tariq, Jay Chen, and Barath Raghavan. ACM Workshop on Hot Topics in Networks (HotNets). 2017.

On the one hand, the concentration of control in a few platforms makes it convenient for governments to censor the Internet *through* them.[334] On the other hand, these giant platforms can implement arbitrary, unaudited policies (possibly unintentionally, e.g. due to discriminatory algorithms) to control how users access and interact with online information. Majority of these platforms provide bottleneck services over the Internet related to web hosting, security, analytics etc. As a result, their policies trickle down to thousands of their client websites. In my study[335] of the Web's differential treatment of users of Tor anonymity tool, I found that majority of such practices are due to two major Cloud Hosting Providers (Akamai and Cloudflare). Their policy extends to all the client websites that they host, effectively leading to an amplified effect.

September 2018

[334] "SoK: Making Sense of Censorship Resistance Systems". Shehar Bano, Tariq Elahi, Laurent Simon, Colleen Swanson, Steven J. Murdoch and Ian Goldberg. Proceedings on Privacy Enhancing Technologies, Vol. 2016, No. 4 (PETS), 2016.

[335] "Do You See What I See? Differential Treatment of Anonymous Users". Shehar Bano, David Fifield, Sadia Afroz,Mobin Javed, Srikanth Sundaresan, Vern Paxson, Steven J. Murdoch, and Damon McCoy. The Network and Distributed System Security Symposium (NDSS), 2016.

BASCA – written evidence (IRN0027)

The Internet: to regulate or not to regulate?

1 The British Academy of Songwriters, Composers & Authors (BASCA) is the professional association for music writers and exists to celebrate, support and protect the professional interests of all writers of music from song writing to media, contemporary classical to jazz.

2 We are an entirely self-funding, not for-profit membership organisation with a history traced back to 1944. Whilst we are well known for putting on the British Composer Awards, the Gold Badge Awards and The Ivors every year, there is far more to us than these events. BASCA campaigns in the UK, Europe and throughout the world in order to protect the professional interests of our members.

3 We count on the best songwriting and composing talent in order to do this important work and are entirely self-funding, relying on the continuing support of our members, who include Sir Paul McCartney, The 1975, Calvin Harris, Coldplay, Dizzee Rascal, Annie Lennox, Gary Barlow, David Arnold, Sir Elton John, Imogen Heap, Howard Goodall, John Powell, Harrison Birtwistle, Kate Bush and many more.

4 The UK music industry grew by 6% in 2016 to contribute £4.4 billion to the economy and musicians, songwriters and composers created over half of that value; contributing just over £2billion[336], £964 million of it in exports. Without the works written by BASCA's songwriters and composers the UK music industry would cease to exist.

Rule of Law

5 We believe internet companies should be bound by the laws and requirements that otherwise bind actors engaged in similar conduct in the offline environment. We must hold internet actors accountable and demand performance that meets the moral and social imperatives of the nation. For far too long, we have treated the internet as a space on the fringes of the jurisdiction of the law. We welcome Government's stated aim in its Digital Charter to align "the same rights and expect the same behaviour online as we do offline".

6 We have also welcomed stricter legislation and enforcement implemented over the past 5 years. The City of London Police Unit (PIPCU) has been a great ally of the creative community in trying to address unscrupulous practices. Since the unit launched in September 2013, PIPCU has been tackling copyright infringing sites in the UK to help protect the creative industries, including music. In 2015 PIPCU diverted over 10.3 million illegal music and film sites to an official

[336] https://www.ukmusic.org/research/measuring-music-2017/

police warning page, suspended over 5,500 websites selling fake luxury branded goods, and seized over £3.5million worth of fake goods[337].

7 This is excellent work in helping to tackle Intellectual Property crime and Government should ensure that they continue to have adequate funding to continue to address what has become a far too acceptable practice of monetising infringement and undervaluing creativity. BASCA also welcomed the raising to 10 years as the maximum penalty for online copyright infringement which now aligns with those applied to the physical world[338].

8 However despite this good work there are major gaps in internet regulation that allow damaging activities to flourish. These are outlined below.

Illegal Listings in Search Engines

9 Despite some voluntary measures from the search engines to downgrade illegal content piracy is more prevalent than ever. Muso recorded more than 300 billion visits to pirate sites last year alone. This is an increase of 1.6 percent compared to 2016[339]. 9 billion of these visits were from UK residents.

10 BASCA would support a duty of care on search engines to prioritise licensed sites in search results, de-list infringing sites and cease auto-complete search suggestions for infringing content. This would also include the Google service "Google Alert" which is notorious for recommending sites hosting illegal content. By exposing users with millions of illegal access to copyrighted works, it sabotages the sources creators use to make a living through a fair music marketplace.

Safe Harbour

11 At the time of adoption of Safe Harbours in the US (Digital Millennium Copyright Act 1998) and UK (via the EU e-Commerce Directive 2000), there was an understandable desire to protect nascent internet platforms, which at the time were little more than bulletin boards. Safe Harbours were intended to foster an environment in which online companies could flourish economically.

12 According to recent reports, YouTube is now one of the wealthiest companies in the world, with a value of approximately $70 billion dollars[340]. YouTube has built its wealth on musical works and yet the money it pays out to the music industry does not reflect its true worth – paying only £25.5 million to the UK music industry in 2016[341]. Safe Harbour has allowed major commercial companies like YouTube and other sites dependent upon User Uploaded Content

[337] https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/pipcu-news/Pages/PIPCU-announces-over-10-million-website-diversions-as-industry-marks-World-IP-Day-2015.aspx

[338] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/517528/Government_Consultation_Response_Criminal_Sanctions_-_Accessi....pdf

[339] https://torrentfreak.com/online-piracy-is-more-popular-than-ever-research-suggests-180321/

[340] https://www.billboard.com/articles/business/6582783/youtube-is-worth-70-billion-on-its-own-says-boa-analysts

[341] https://www.theguardian.com/business/2017/apr/15/music-industry-youtube-video-streaming-royalties

(UUC) to operate on so-called "DMCA licenses" which is to say, no license or severely under-licensed. This is what we refer to as the value gap.

13 We therefore welcome the proposals outlined in the draft EU Copyright Directive [342] which aim to address the blatant misuse of Safe Harbours by re-defining what platforms can rightly claim to be passive hosts. We hope this legislation will pass through the European Parliament and be enacted into British law before we exit the European Union.

Notice and Stay Down

14 These platforms also avoid responsibility for trafficking in piracy by their methodology of only removing specific infringing files when notified. Google, owner of YouTube, now processes around 75 million take-down notices each month[343]. This is a clear example of a broken system.

15 We support their taking action to avoid unauthorised content on their platforms by putting in place content recognition technologies. However, works need to stay down once a notice has been verified, referred to as "notice and stay down". This would guarantee illegal content stays down once notice is given, as opposed to merely being taken down temporarily only to be re-hosted immediately by the same or another infringing party. This would assist in not just removing more illegal uses of music on platforms but also other illegal content such as terrorist propaganda.

16 The current situation places the copyright owner, often an independent songwriter or composer, under a constant time and financial burden to keep policing the same content on the same sites. The rightsholder can spend many hours a day monitoring their works or the alternative is paying for a technological solution. Both of these options reduce the ability for self-employed songwriters and composers to earn an income. Notice and stay down would be a huge benefit and technologically, an easy system for hosting sites to implement.

Conclusion

17 Copyright is the foundation of the music industry. It allows companies to invest in talent and musicians and composers to make a living. We welcome the broad aims of the Government's Digital Charter but note that its first aim of growing technology companies must not come at the expense of the music industry. Reducing enforcement of copyright at the expense of rightsholders for the benefit of the tech industry does not make economic or moral sense. Should internet services and platforms be freed from the responsibilities of all other actors? We would question whether this even needs to be asked.

[342] https://www.reedsmith.com/en/perspectives/2017/06/european-copyright-reform-safe-harbour-and-the-value-gap

[343] https://www.bizjournals.com/sanjose/news/2016/03/07/how-many-copyright-takedown-notices-does-google.html

We have welcomed the opportunity to be able to share with you our position.

10 May 2018

BBC – written evidence (IRN0102)

Introduction

1. The BBC welcomes the opportunity to submit evidence to the House of Lords Communications Committee's inquiry into internet regulation.

2. The BBC is submitting evidence to this inquiry as a public service broadcaster (PSB), an organisation that provides world-class, impartial and accurate news and a major provider of internet content and services. We have addressed the areas which are most relevant to the BBC.

3. The BBC has a public mission to inform, educate and entertain. We recognise that the internet has significant potential to help us fulfil this mission. It enables people to be more creative, more connected and more engaged in political, economic and cultural life, in accordance with the original intentions of its creator, who "imagined the web as an open platform that would allow everyone, everywhere to share information, access opportunities, and collaborate across geographic and cultural boundaries."[344]

4. This open platform has changed the market quickly and definitively, with the result that audiences now have more choice across both television and audio services than ever before. However, the speed of these changes has also created challenges for legislation and regulation including the spread of misinformation (fake news) and the misuse of data.

5. We have grouped our response into four key areas: the Government's Digital Charter, content regulation, changing audience habits, and business practices.

Digital Charter

6. The Government said that it intends to tackle some of the issues around internet regulation through its **Digital Charter**. We welcome the Charter as an important opportunity to:

   - identify the guiding principles for Government, industry and civil society groups, that can act as a reference point for now and in the future, and

   - in so doing, provide certainty to digital businesses as a significant proportion of its regulatory context shifts from EU into UK law, including some principles fundamental to effective competition.

[344] Tim Berners Lee, https://www.theguardian.com/technology/2017/mar/11/tim-berners-lee-web-inventor-save-internet

7. We welcome the Secretary of State for Digital, Culture, Media and Sport's intention to, "work with publishers, tech companies, civil society and others to establish a new framework that protects users and their rights online and offers opportunities alongside obligations for businesses and platforms."[345] The BBC is happy to play its role in developing this framework.

Content regulation

8. The BBC is subject to strict regulation of content by Ofcom. All BBC content – whether broadcast, online or on BBC channels on social media platforms – is governed by our Editorial Guidelines.[346] There are three key areas which highlight the differing standards between internet and broadcast content: online harassment and abuse, fake news and protection of children.

Online harassment and abuse

9. The internet enables greater immediacy of contact with people across the world but can also be used as a vehicle for unacceptable and criminal behaviour. BBC journalists, particularly women, have been subjected to online harassment.[347] This demonstrates that some issues may not be remedied without robust legal and regulatory frameworks.

10. The Chair of the BBC, Sir David Clementi, previously stated "I welcome the work the government is doing to tackle this, and I'm following closely the efforts of Twitter and Facebook, amongst others, to clamp down on the perpetrators. I hope the social media platforms do even more."[348]

Fake news

11. The BBC defines fake news as false information deliberately circulated to misinform, usually for political or commercial purposes. The internet has enabled people to receive fake news and share it with a wide audience quickly. A Council of Europe report likened the spread of this misinformation to pollution.[349]

[345] https://www.digitaltveurope.com/2018/03/13/uk-government-calls-for-digital-platforms-to-step-up-online-rules/

[346] http://www.bbc.co.uk/editorialguidelines/

[347] A study by Demos found that Journalism is the only category where women received more abuse than men, with female journalists and TV news presenters receiving roughly three times as much abuse as their male counterparts. https://www.demos.co.uk/press-release/demos-male-celebrities-receive-more-abuse-on-twitter-than-women-2/

[348] http://www.bbc.co.uk/mediacentre/speeches/2017/david-clementi-cambridge

[349] https://www.coe.int/en/web/freedom-expression/news/-/asset_publisher/thFVuWFiT2Lk/content/tackling-disinformation-in-the-global-media-environment-new-council-of-europe-report?_101_INSTANCE_thFVuWFiT2Lk_viewMode=view/

12. The 2018 Edelman Trust Barometer[350] showed that less than a quarter of the population trusted social media as a source for news and information.[351] In comparison, the BBC is the most trusted source of news in the UK by far (TV broadcaster, radio, newspaper, magazine or website) and one of the most trusted worldwide. The Secretary of State for Digital, Culture, Media and Sport told the House of Lords Committee on Political Polling and Digital Media that "One of the most significant things we have in the UK to protect us against [fake news and interference in social media] is the BBC … The case for high-quality BBC news and for the licence fee has significantly strengthened over the last decade or so, with the rise of social media."[352] In an age of fake news, this is a responsibility we take very seriously.

13. The BBC's Royal Charter sets out our five public purposes, the first of which is "To provide impartial news and information to help people understand and engage with the world around them".[353] BBC research shows that around 80% of UK adults use BBC News every week.

14. In accordance with the BBC's Editorial Guidelines[354], we are committed to achieving due accuracy and impartiality and to being rigorous in establishing the truth of the story. Editors are trained to spot fake news and the BBC established a User Generated Content (UGC) Hub more than a decade ago to provide dedicated eyewitness verification in the newsroom.

15. The BBC also runs initiatives to tackle fake news. This includes Reality Check[355], which challenges misleading statements from public figures online and on TV, and a national training programme as part of the BBC's School Report scheme which will help young people identify real news and filter out false information. The scheme will see up to 1,000 schools offered mentoring in class and online.[356] BBC Trending is a service that looks to unpick the truth behind the stories emerging on social media.[357]

16. Beyond the BBC, fake news has highlighted issues with platforms such as Facebook, Google and Twitter, which have tended to provide unmediated access to large audiences to this material. We welcome attempts to tackle misinformation by the platforms themselves. However, we are mindful of the potential unintended consequences of some policies. For example, when YouTube announced its intention to label video content by publicly-funded broadcasters and broadcasters who are fully or

[350] The 2018 Trust Barometer is Edelman's 18th annual trust and credibility survey, measuring trust across a number of institutions, sectors and geographies. The Trust Barometer surveys more than 33,000 respondents across 28 countries.

[351] https://www.edelman.co.uk/magazine/posts/edelman-trust-barometer-2018/undefined

[352] Evidence to the House of Lords Select Committee on Political Polling and Digital Media, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/political-polling-and-digital-media-committee/political-polling-and-digital-media/oral/75964.pdf

[353] https://www.gov.uk/government/publications/bbc-charter-and-framework-agreement

[354] http://www.bbc.co.uk/editorialguidelines/guidelines

[355] http://www.bbc.co.uk/news/topics/cp7r8vgl2rgt/reality-check

[356] http://www.bbc.co.uk/news/resources/idt-8760dd58-84f9-4c98-ade2-590562670096

[357] http://www.bbc.co.uk/news/blogs/trending

partially funded by government[358], it was criticised for conflating content from editorially-independent public broadcasters with state-sponsored news.[359]

17. The BBC submitted written evidence to the Digital, Culture, Media and Sport inquiry on fake news.[360] We await the findings and policy proposals to tackle the issue.

Children's content and services

18. The BBC sets a gold-standard in the provision of online services and content for children in the UK. This was acknowledged by government in the Internet Safety Strategy Green Paper, which states that the BBC's online services provide a "safe, trusted space where [children] can learn, create and have fun in one place … We will engage with the BBC as they support and promote child online safety and digital literacy through BBC Children's Stay Safe initiative, helping UK children become among the most digitally literate and resilient in the world."[361]

19. As outlined in the BBC's submission to the Committee's *Children and the internet* inquiry,[362] this is delivered predominantly through the BBC's policies rather than external regulation, though we are accountable to Ofcom for the protection of under-18s in our licence fee-funded television and radio services.[363]

20. Any industry organisation providing digital services to children should provide information for parents and users about how to engage with the company's services safely. Our guiding principle is that it is for parents to oversee the consumption of our online and digital content but it is our responsibility to provide children and parents with access to the content, information and tools to make these decisions. We deliver this through: our Editorial Guidelines; design of apps and other services; and advice and guidance.

21. All BBC content – whether broadcast, online or on BBC channels on social media – is governed by our Editorial Guidelines. These include substantial policies and advice on child protection. We also have very clear guidance about what should appear on the BBC online – for example, any content on or one-click away from the BBC Home page would normally be suitable for a general audience.

[358] https://youtube.googleblog.com/2018/02/greater-transparency-for-users-around.html
[359] https://www.washingtonpost.com/news/the-switch/wp/2018/02/03/youtubes-new-attempt-to-limit-propaganda-draws-fire-from-pbs/?noredirect=on&utm_term=.a1f2901cf154
[360] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/culture-media-and-sport-committee/fake-news/written/48758.html
[361] https://www.gov.uk/government/consultations/internet-safety-strategy-green-paper p33
[362] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/communications-committee/children-and-the-internet/written/40400.html
[363] http://www.bbc.co.uk/editorialguidelines/guidelines/accountability/ofcom

22. BBC apps and other online services for children are designed with appropriate safeguards in place. For example, the new CBBC Buzz app[364] has a team of moderators to approve or decline user-generated content, extensive parental controls and no means to make negative comments about other users' content.

23. Online services such as iPlayer have protection systems such as G for Guidance, which not only provides a parental lock, but also offers programme information which replicates the information available for post watershed programmes on TV. When this system was introduced it was offered it to the other UK national PSBs, with the help of Ofcom, which enabled all UK PSBs to have the same system of guidance and pin protection. We also use the G for Guidance principles and labelling for our off platform on demand content. We aim to ensure that our judgement on guidance warnings is as up to date as possible, particularly on language, following Ofcom research on changing perceptions on offensive language.

24. The BBC is also a UK-leader in providing advice and guidance to children and their parents on how to navigate online. This includes the *Own It*[365] website (developed from the Stay Safe initiative) which collates BBC and third-party resources for 9-12 year olds to help them stay safe and enjoy their time online.

25. In contrast to the safe online spaces provided by the BBC, BBC research shows that children and young people have been exposed to negative, harmful or inappropriate content online. One in six 12-15 year olds and one in ten 8-11 year olds who go online had seen something in the past year that was worrying, nasty or offensive.[366] Recent revelations that YouTube Kids contained inappropriate content have further underlined the need for appropriate safeguards for children online.[367]

26. A further issue is social media, which is the central experience for many children online. Social media organisations are almost exclusively US-based and therefore subject to COPPA, which sets the minimum age for participation at 13 years. The EU GDPR suggested an age limit of 16 but left it to the discretion of member states. The UK has kept the minimum age at 13. The BBC is clear that we will not target children under 13 and is very careful about how we respond to children age 13 – 16 online. However, a BBC survey suggested that more than two thirds of 10 – 12 year-olds have a social media account.[368]

27. We welcome the opportunity to advise Government and other partners on our experience of establishing best practice for children's content and services online.

[364] http://www.bbc.co.uk/mediacentre/latestnews/2018/cbbc-buzz]

[365] https://www.bbc.com/ownit

[366] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/communications-committee/children-and-the-internet/written/40400.pdf

[367] http://www.bbc.co.uk/news/technology-43893862].

[368] http://www.bbc.co.uk/news/education-35524429

Social media levy

28. The 2017 Conservative manifesto pledged to introduce a levy on "social media companies and communication service providers" to fund greater public awareness of online safety and preventative measures to counter internet harms.[369] As Government is considering how levy funds might be used to generate maximum impact, the BBC would be happy to share its thinking, for example looking at what strategies can deliver the greatest reach, measurable value amongst the target user group (i.e. awareness, behaviour change, user recognition), and efficiency.

Changing audience habits

29. The way people consume content is changing, particularly among the younger demographic, as audiences shift increasingly to online and on-demand content. This development has created challenges in the regulatory system, as the speed of technological development has overtaken legislation and regulation. There is a specific regulatory challenge for the BBC over PSB prominence, along with wider issues of funding, provision of access services and support for digital terrestrial television (DTT).

30. The BBC provides extensive online services, including iPlayer, BBC News Online and apps. During this Charter, we will increasingly serve two audiences: those who largely use broadcast services and those who access the majority of our content online. We are highly innovative online, in line with our Charter obligation to support technological innovation.

31. The emergence of on-demand services such as Netflix and Amazon Prime has led to an increasingly competitive market for content, talent and resources. PSBs now compete directly for content with a range of new providers, including globally-focused pay operators.

32. A study commissioned by the BBC found that audience consumption habits are changing, particularly amongst younger age groups who "are more likely than the average to subscribe to SVOD [Subscription Video on Demand] services, to use portable connected devices and to view content other than at the time of the broadcaster's choosing."[370] These younger age groups are essential to the future of public service broadcasting.

33. This represents a challenge, not just for the BBC but for the wider creative industries in the UK. In order to meet this challenge the BBC's Director-General Lord Hall has indicated that partnerships will be increasingly important, "we're going to have to work with others like never before – working with the big tech companies like Google, learning

[369] https://www.conservatives.com/manifesto
[370] http://downloads.bbc.co.uk/aboutthebbc/insidethebbc/howwework/reports/pdf/content_market_dynamics.pdf

from them, building on what we're already doing together, to get what we do to as many people as possible."[371]

Increasing importance of prominence and attribution

34. The current PSB prominence regime was introduced in the Communications Act 2003 and has not kept pace with technological and market change. It created PSB prominence regulation for broadcast TV sets but not for connected TV sets, and for the existing PSB channels but not PSB on-demand players. With a big shift occurring towards on-demand and online consumption, a regulatory imbalance has become increasingly clear.

35. The primary PSB services[372] continue to deliver half of all viewing within both linear broadcast and catch-up TV, but changing patterns of consumption could make the existing prominence protections less relevant over time.[373]

36. The fragmentation of viewing across different platforms can make it difficult to find PSB content. PSBs have developed award-winning on-demand players, such as BBC iPlayer, but these are outside the scope of prominence rules. There are now a myriad of ways in which audiences can consume TV via the internet, many of which have advanced search and personalised recommendation models. As noted by Ofcom "Modern user interfaces … can promote on-demand content and box sets based on viewers' past choices, ahead of linear broadcast channels."[374]

37. We welcome the Ofcom commitments to "seek to ensure the widest availability and prominence of PSB"[375] and to "ensure the main PSBs will remain prominent, and ensure the smaller PSBs get more visibility, and provide more detailed guidance to ensure that rules can be enforced."[376] We look forward to the regulator's recommendations following the forthcoming consultation on updates to the Code underpinning electronic programme guides.

38. We would urge clarity from Government and Ofcom in their respective roles in ensuring future prominence for PSBs online, particularly in light of Ofcom's statement that "if Parliament believes the future health of PSBs requires prominence in on-demand services, it would need to pass new legislation."[377]

Challenges to funding

[371] http://www.bbc.co.uk/mediacentre/speeches/2018/tony-hall-annual-plan

[372] BBC, ITV, Channel 4 and Channel 5

[373] http://downloads.bbc.co.uk/aboutthebbc/insidethebbc/howwework/reports/pdf/content_market_dynamics.pdf

[374] https://www.ofcom.org.uk/__data/assets/pdf_file/0026/111896/Public-service-broadcasting-in-the-digital-age.pdf

[375] https://www.ofcom.org.uk/__data/assets/pdf_file/0026/111896/Public-service-broadcasting-in-the-digital-age.pdf

[376] Sharon White speech to Enders conference, https://www.deloitte.co.uk/mediatelecomsbeyond/

[377] Sharon White speech to Enders conference, https://www.deloitte.co.uk/mediatelecomsbeyond/

39. Alongside the regulatory gaps created by increasing online and on-demand content, the BBC also faces funding challenges. A study commissioned by the BBC predicted, assuming a constant ratio of UK originations spend to revenues of 20% for traditional funders, a potential gap in expenditure in real terms of more than £500m on original content by 2026 (enough to fund 230 episodes of *Sherlock* or 700 episodes of *Vera*).[378]

40. BBC research shows that these trends are set to continue. Over the next ten years we expect a very substantial gap to open up between the amount that is spent on UK content now and the amount that will be spent in the future. This gap would be even greater if the licence fee were to decline. The impact of this could be the gradual loss of content which would have serious implications for the BBC to deliver on its public purposes and the wider PSB sector to deliver on its aims.

41. A key challenge for the BBC is how to fulfil its mission and public purposes during this shift from linear broadcasting to on-demand. We are urgently working on solutions and responses to these challenges such as the improvement of the iPlayer and BBC Radio.

Access services

42. The switch from linear to on-demand could have a disproportionate impact on certain sections of viewers. The BBC has a strong track record in pioneering access service provision for both linear and on-demand. For example, since 2012, we have made 100% of programmes from our main channels available on-demand with subtitles via BBC iPlayer. The BBC's track-record has also been recognised by leading disability rights charities.[379]

43. Ofcom has identified the gap in provision of access services by on-demand service providers compared to broadcast channels[380] and is currently consulting on proposed changes to the access services regime. We have recommended that, in the case of Video on Demand only On Demand Programme Services, Ofcom should test whether the interests of audiences would merit further regulation. We also recommend they consider the impact of jurisdictional limitations in relation to access service provision, subject to proportionality checks and audience interest.

The internet and the mixed economy of TV and radio distribution

[378] Mediatique, *Content market dynamics in the UK: outcomes and implications* http://downloads.bbc.co.uk/aboutthebbc/insidethebbc/howwework/reports/pdf/content_market_dynamics.pdf

[379] In Charter Review for example, Action on Hearing Loss stated that *'the BBC to date has played an extremely important role within the broadcasting industry in promoting accessibility'*.

[380] Only 36% of on-demand service providers offer subtitles, 11% offer audio description and 4.5% signing

44. Within and throughout the mandate of its 11 year Royal Charter, the BBC remains committed to serving all audiences whether they are already enjoying the benefits offered by internet or are using the BBC's popular broadcast services.

45. The BBC recognises the important role that broadcast services, including DTT, continue to play for many audiences, and the importance of maintaining adequate spectrum to serve it while that remains the case. Similarly, the BBC has invested significantly in DAB. We remain of the view that DAB is very important but only as a part of the story, along with FM and IP. For both TV and radio services, the BBC remains committed to a transition at the pace of the audience and to ensuring it leaves no audiences behind.

46. As part of this, the BBC will continue its dialogue with audiences and with partners across the TV and radio industries in particular, including the BBC's joint ventures and the third party distribution platforms to whom the BBC makes its services available.

Business practices

47. The recent focus on Facebook and Cambridge Analytica has demonstrated an increased awareness of and need for online platforms to be transparent about their business practices and use of personal data.

Data

48. It is widely acknowledged that the collection and analysis of data is important to provide a personalised service. In the future, the BBC will need to make the most of the opportunities offered by IP delivery to get more, better, personalised content and services to audiences in order to sustain a thriving UK creative economy. However, the BBC believes that individuals should have ownership and control over the data collected from them directly or indirectly. The BBC's data policies are clear, transparent and available to read online.[381]

49. We note the current proposed EU Regulation regarding the 'promotion of fairness and transparency in online intermediated trade', which aims to create a fair balance on data transparency between platforms and businesses.[382] Access to data is also vital to enable the BBC to deliver its public purposes.

Artificial Intelligence

50. There should be greater understanding of how the use of AI and personal data affects people. When personal data is used by AI to make decisions that will impact an individual, then it should be the right of an individual

[381] https://www.bbc.co.uk/usingthebbc/privacy-policy/

[382] https://ec.europa.eu/info/law/better-regulation/initiatives/com-2018-238_en

to understand on what basis decisions about them are made. As stated in our response to the House of Lords Committee on Artificial Intelligence, research presented at the Leverhulme Centre for the Future of Intelligence has shown it is possible to expose the characteristics of the decision-making process without needing to peer into the black-box – that is, it is possible to offer algorithmic transparency without having to compromise intellectual property. [383]

51. The predictive and analytic capabilities of AI to complete a web search, automatically respond to messages, or to offer personalised recommendations is well documented. However, AI systems that shape and direct the public's attention risk straying into social engineering. AI will come to control the information we see and the choices offered to us, and there is real worry over the role AI (and the organisations controlling AI services) will play in shaping the norms and values of society.

52. The UK can be a leader in this field provided we are guided by public interest. The BBC can play a critical role in the development of beneficial AI both technically, through the development of AI services, and editorially, by encouraging informed and balanced debate. The BBC has adopted four principles regarding the use and development of AI, which we recommend are adapted and adopted by others: independence, impartiality, accountability, universality.

Voice command and recognition

53. Voice command and recognition systems are likely to become increasingly important as means for audiences to discover content and information. Therefore the systems which control these devices, such as algorithms, business practices and governance, will become more important too. PSB has had a direct, unmediated relationship between broadcasters and audiences. This has enabled it to deliver qualities and attributes to the audience that have been created and nurtured over decades, such as quality, breadth and universality.

54. The increase in use of technology such as voice could pose a challenge to these values and the resulting contribution of PSB to society. We need to ensure that these attributes of broadcasting are not only carried over into the digital age but that they are amplified by the creative potential of the internet.

Net neutrality

55. Net neutrality is a foundation for fair market competition, preventing Internet Service Providers (ISPs), who are increasingly investing in their own content services, from 'throttling' other content providers' offers. We welcome Ofcom's role in monitoring market developments and

[383] http://lcfi.ac.uk/about/ https://www.parliament.uk/documents/lords-committees/Artificial-Intelligence/AI-Written-Evidence-Volume.pdf

compliance in relation to net neutrality laws in light of international regulatory trends and fast-developing business models.

56. This is supported, in principle, by providers ranging from Microsoft, Netflix, and the BBC to online retailers, health care providers, universities and libraries. Without it, the ISPs have the potential to exploit their gatekeeper power to the detriment of competition.

57. The BBC would welcome a Government commitment to protect net neutrality, currently guaranteed by EU Regulation but soon to transfer into UK law under the EU Withdrawal Bill.

June 2018

BBC, Channel 4 and ITV – oral evidence (QQ 143-151)

Tuesday 16 October 2018

Watch the meeting

Members present: Lord Gilbert of Panteg (Chairman); Baroness Benjamin; Baroness Bertin; Baroness Bonham-Carter of Yarnbury; The Lord Bishop of Chelmsford; Baroness Chisholm of Owlpen; Viscount Colville of Culross; Lord Goodlad; Lord Gordon of Strathblane.

Evidence Session No. 17 Heard in Public Questions 143 - 151

Examination of witnesses

Dan Brooke, Chief Marketing and Communications Officer Channel 4; Magnus Brooke, Director of Policy and Regulatory Affairs, ITV; Clare Sumner CBE, Director, Policy, BBC.

Q143 **The Chairman:** I would like to welcome our witnesses to our House of Lords inquiry into regulation of the internet. Our witnesses today are from the broadcasting companies. You are very welcome. Thank you for taking the time to come and give evidence. In a moment I will ask you to say a few words of introduction. Today's session will be recorded and a transcript will be kept. We may have a Division or possibly several Divisions during the session this afternoon. If that happens—one of them may come quite soon—we will briefly suspend the session for about 10 minutes and then come back and pick up where we left off.

Our witnesses are Dan Brooke of Channel 4, Magnus Brooke from ITV and Clare Sumner of the BBC. May I ask the witnesses to briefly introduce themselves, tell us about their role and about any perspectives they have on the broader issue that the Committee is investigating. In so doing, please tell us what you think are the strengths and weaknesses of the regulated framework for the internet and particularly if your organisations have an assessment of the Ofcom report regarding harmful online content, which you will all be aware of.

Magnus Brooke: I am director of policy and regulatory affairs at ITV and I am responsible for our relations with Ofcom, with Government and with the European institutions. It is important to begin by recognising the incredible benefits that the internet and many of the major online businesses have brought to people's lives. The process that we have seen in the development of the internet, however, is a bit like 19th century industrialisation. In both cases, we have seen rapid growth and transformation unconstrained by specific regulatory restrictions, but at the same time we have seen significant externalities. It took some time for Government to catch up with industrialisation and to do something about it and the externalities. I do not think that we should repeat that mistake.

Beyond the general law, there is very little specific regulation for major online platforms. Indeed, it is the reverse; laws were put in place at the outset to avoid those platforms assuming real liability. Whereas that was once a strength, it now looks unsustainable. To put it into perspective, if you think about a chemical plant or an oil refinery, they do important work but there is clear agreement that they cannot pollute rivers or groundwater near to them with waste products. It is the cost of doing business to make sure that those waste products and processes are dealt with effectively and appropriately. This is not voluntary. It is not on a best-efforts basis. It is a mandatory legal requirement. We need to start tackling the downsides of major online platforms in the same way.

On the Ofcom contribution, we thought it was considered and helpful. We were struck by Ofcom's research into the scale of online harm. We also thought that its highlighting of a lack of a level playing field between people like us and some of the new online platforms was also helpful. Above all, its suggestion that there are things that you can learn from the broadcasting sector and apply to online was helpful, particularly the idea that Parliament sets a clear statutory objective of the kinds of harm that the regime is seeking to prevent and where an independent body such as Ofcom is instructed to establish an effective regime on the back of that.

Then, with powers of enforcement, it is a matter for the platforms to comply, just as we comply as broadcasters. We can see no reason why that approach would not work. Ofcom already oversees a system in which there is a need for appropriate levels of protection and assurance against harmful content, but it also recognises the potential conflict between that and freedom of expression. It is well equipped and experienced in dealing with that potential conflict, as we are as broadcasters.

Clare Sumner: I am a director of policy for the BBC and my remit covers very similar areas to Magnus, so I will not repeat it. As I was preparing for this Committee, I thought I should go back to Sir Tim Berners-Lee. We were all very excited at the beginning by the opportunities of the web for freedom of expression and creativity. I was struck that he said recently, "The responsibility—and sometimes burden—of making these decisions falls on companies that have been built to maximise profit more than to maximise social good. A legal or regulatory framework that accounts for social objectives may help ease those tensions". That is something that the Committee should have in mind.

We have said before in relation to the BBC that the current regulatory system has an imbalance. This may not just be in the UK; there may now be a global imbalance. It is definitely the right time for your Committee to look at this, and we believe that a stronger framework is needed.

We also think that in this context you should also consider the role of the PSBs and help to ensure that this important part of the UK creative economy continues to thrive. The imbalance that we see at the moment is in a tightly regulated PSB system. In many ways that is right because of our accountability, the way we are funded and the importance of transparency. However, we are also seeing an imbalance with new market players who are now operating in a very different space and in a very different way. As you know, as part of this the BBC, ITV and Channel 4 have been campaigning for things like the importance of prominence so that people can find PSB content easily. I would particularly flag the importance of attribution and well-sourced news, which are critical in the battle against fake news.

Picking up on the Ofcom report in particular, there were three things that really struck me. First, many of our audiences and consumers think that YouTube is much more highly regulated than it is; 30% thought that it was already covered by regulation. It is a concern that people think that they are consuming something with set principles and standards when in reality we know that not to be true.

Secondly, I commend page 18 of the report to you. I have brought it with me. This is a diagram which shows you that different kinds of organisations with exactly the same content are treated in different ways. That reinforces my point about the imbalance at the moment in the current system.

Finally, on the framework that has operated so successfully in this country, like Magnus—I suspect we might break out in agreement about this—I think it has been about Parliament creating a framework of principles and a framework of standards for what is important. In order to have a good regulatory system you need two things. First, you need the organisations themselves to create standards. For the BBC, I would flag up the world-leading editorial standards. Part of the reason why that is so important is that you then get a culture in the organisation that applies to those standards. Things such as complaints and appeals and regulatory backstops are the last resort.

The question in this debate, however, is: what is that backstop? The Committee needs to look at this. What is that sanction that encourages organisations to change some of their ethos and their culture and therefore operate in different ways to deal with the harms, which I know the Committee has already taken a lot of evidence on so I will not repeat them? Briefly, as you know, there is the social impact on children, bullying, harassment, hate crime, and this huge issue with fake news.

Dan Brooke: Thank you for the opportunity to give evidence. I am the chief marketing and communications officer for Channel 4, which incorporates corporate affairs. I am also the board champion at Channel 4 for diversity and inclusion, which is a role that I am particularly proud to hold.

I would echo much of what Magnus and Clare have said. I will start with the positives, which are always a good place to start in life. The internet is arguably humankind’s greatest ever invention. It has transformed life in the world in so many ways across so many different fields, in parliaments, in governments, in business and the media. The list goes on. There are unfortunately dark sides, and sadly those dark sides are considerably more significant than my children’s obsession with the game “Fortnite”, which they spend a considerable number of hours of their day on. We are talking about trolling. We are talking about fraud, cyberbullying, hate speech, child abuse, fake news, and so on. I am sure these are not intended consequences of the internet, but they are undoubtedly consequences, and the system that we have in place, however we choose to describe it, has not prevented those things.

I would ask whether there is a problem and how big the problem is. The answer to that question is that we do not know. When we have the chief executive of NHS England talking, as he did last week, about the problem with young people submitting themselves to the health service for mental health complaints as a result of using social media, which is reaching epidemic proportions, we can safely say that we have a problem.

All those things that I mention are, of course, grave concerns, but our belief is that the most insidious one is fake news. Why? Because fake news undermines the fundamentals of how we choose to organise ourselves as a society through the system of democracy. We believe that information is the lifeblood of democracy and that fake news is like leukaemia. It is like a cancer to the blood supply of democracy. It is absolutely essential, and we applaud the fact that Parliament is looking into it and how to regulate the internet better.

As an organisation and a public service broadcaster, we are looking into it. Last year we held a week called Fake News Week. This year we have had our Channel 4 News exposé of the operations of Cambridge Analytica and a "Dispatches" programme that went undercover in a Facebook moderation centre. We will continue to do these things.

I would like to conclude by echoing what Clare said about thinking hard about how to cherish and nurture the positive side of the system. As we would perceive it, this is the side of the system that is putting something positive into the blood supply by way of public service news and cherishing the system that produces it, in particular by focusing on updating and modernising these rules on prominence.

The Chairman: Thank you to our witnesses who have covered a lot of ground. We will return some of these areas in our questions, the first of which will come from Baroness Chisholm.

Q144 **Baroness Chisholm of Owlpen:** Welcome. I am interested that it has been mentioned that it would be a good idea to have the establishment of a new horizon-scanning or possibly even a co-ordinating body. Would that help the regulators?

Dan Brooke: Yes. On the Ofcom report, the co-ordination that it already has with the ICO, the Electoral Commission and the CMA seems very positive. I know that the Commons Select Committee has recommended much more co-ordination between those bodies, and that is important. We believe that the issue of content delivered on the internet is so vast and so absent largely of regulation at the moment that a body that is specifically dedicated to that is imperative. It is entirely possible that one could get to a position where it is best placed as a specific unit within an existing regulator like Ofcom. Because of the vastness of what such a body would have to look at, what might make sense is for that body to have the co-ordinating role between all the other regulators that touch on activities on the internet.

The Chairman: Would you prefer Ofcom to take on that co-ordinating responsibility if it were clearly defined, or do you favour a new body to bring it together?

Dan Brooke: We favour a body that is dedicated to the subject of content regulation. As to whether that is a separate body from Ofcom or that sits within Ofcom, we do not at this stage have a strong view. Wherever it sits, we believe that it should have a strong co-ordinating role with other regulators.

Baroness Chisholm of Owlpen: Presumably one of the points about possibly having a new body would be that it would help the joined-up effect, which does not seem to be happening at the moment between the different platforms.

Clare Sumner: I take a slightly different view on this, partly from my time in government when I worked in the Cabinet Office. I was privileged to work with Lord Hennessy and think about horizon scanning. There is a really important role for government here, because when you get an intervention that is as big as the internet, and if you think about the new interventions, which I know that you have been talking about, such as data and artificial intelligence, and where that takes us in 30 years' time, you are narrowing the question slightly because there are several elements to it.

First, there is a real role for government, whether that is in the Cabinet Office or the DCMS, because the industrial strategy has only fairly recently picked up on the UK creative economy and tech economy. That shows potentially that we need to be doing more in this area. We should probably acknowledge that coming to these issues at this stage feels a bit late for all of us. There is a macro issue, therefore, and precise natures regarding what the regulators should do.

As you know, Sharon White has been open to allowing the issues to be placed on the table. There could be a role for Ofcom and there could be a role for another body. We do not have a strong view on that. I do have a strong view, however, on things that fundamentally change the UK economy and the UK culture; there is definitely a role for government horizon scanning. I agree with Dan that the Government would again be well placed with regard to co-ordination and bringing things together. That is where I come from on this question.

Magnus Brooke: There are two slightly different things going on here. One is the application of the general law to these platforms. There are a number of different regulators of various different sorts applying the general law. There is, however, also a specific question about the content that appears on online platforms, and whether there should be a specific regulatory regime for that content, with a regulator whose responsibilities are defined in statute and backed by effective penalties.

For me, that is the critical question. That organisation could be Ofcom and it could also be the co-ordinating body with a lot of these other regulators seeking to apply the general law. You end up therefore, as you often do in broadcasting, with a sector-specific regime targeted at a particular thing, in our case broadcasting, together with the general law, which is the Information Commissioner's Office, the Gambling Commission and all sorts of other people. There is a degree of co-ordination between those to some extent overseen by Ofcom.

The other point is to make sure that this new regulator, regulatory apparatus or whatever is well resourced. Making sure that the regulator understands the thing it is trying to regulate could be quite expensive. You are trying to recruit quite a lot of people who are well paid and in high demand, so it is important to make sure that the regulator is appropriately funded by some sort of levy from the people it is regulating, as we do with Ofcom. We pay millions of pounds a year to Ofcom and at ITV we do not have any difficulty with that. We want to have a high-quality regulator with good people with whom we can have a high-quality conversation. That is where we should be trying to get to.

The Chairman: Can I come back to Clare on the issue of the role of government with regard to horizon scanning and setting some principles? Do you think that through the Digital Charter programme the Government are doing that or not?

Clare Sumner: I think it meets it in part, because it is a principle-based approach, particularly in relation to harms. The bit that is potentially missing is what the implications will be in 20 or 30 years of some these things and therefore what framework we should consider putting in now to get the outcome that we want in 20 or 30 years. We support the Digital Charter. We think it is a good idea and a good intervention. The question is whether it is sufficient in itself and whether we should go further.

Q145 **Lord Gordon of Strathblane:** This question is particularly for Clare. Any regulatory structure is bound at some point to recommend the need for some degree of further legislation. Do you think that government as we operate now is equipped to deliver that regulation in time, or that by the time the ink is dry on the Act of Parliament we may have moved on to a different technology?

Clare Sumner: That is a good question, and it is one of the things we have been looking at in relation to our campaign on prominence, which is perhaps to give more discretion to a Secretary of State with regard to future changes.

In answer to your question, however, you can protect that partly by having a clear, principled approach. That is the only way you can ensure it. If you get into too much specificity, there is a danger, as you say, that the market moves so quickly and the interventions happen so fast that it could be out of date, which is why you need to be at a high level.

Lord Gordon of Strathblane: You will be aware that MPs in particular, perhaps quite rightly, are very sensitive about giving Ministers powers that are untrammelled and not responsive to parliamentary scrutiny.

Clare Sumner: I absolutely accept that.

Viscount Colville of Culross: Magnus, you spoke about the BBC in your evidence and about the social levy. You talked about ensuring that it generates maximum impact and that you would like to look at a range of different strategies. If you are setting up a new body, making sure that you get the maximum talent to be able to understand what is happening and to horizon scan is going to be incredibly expensive. Will that not take up most of the money from the social levy, or do you see the social levy as having a whole range of different functions?

Magnus Brooke: It depends on what you set up and how you do it. For example, if you gave responsibilities to Ofcom, it is an established organisation and you would not be starting again with a completely new organisation. There is clearly an economy in doing it in that way, and there are certain co-ordination benefits, because these worlds are colliding. The world of broadcasting, the world of YouTube and the world of social media are all coming together. Putting them into an established organisation like Ofcom from the content point of view would make a lot of sense. There is then less pressure potentially on the levy.

In a sense, however, the uses of the levy depend on how big the levy is, we are talking about companies that are making a serious amount of money with a very high margin. We are saying that the externalities that they create in society need to be compensated for. That is the cost of doing business that we all bear and we pay for a regulator. That is the appropriate way to do these things. If there are other projects such as media literacy or other things that the levy could pay for, that is terrific. Ofcom may or may not be the vehicle for deciding that. There may be some other approach to dividing up some of that levy and using it for other public purposes such as the education of children and safety initiatives. There are a number of different things that you could think of. The primary purpose to start with, however, is establishing an effective regulator with a regime that works.

Clare Sumner: I very much agree with that approach. It makes a lot of sense. We probably pay a bit more than ITV because obviously the regulator does more in relation to the new charter for the BBC. It is important that we ensure that the respective platforms are contributing to that high-quality regulation. By doing that, it will ensure that you get the right people looking at these questions. There is a danger that you create further imbalance if you do not set up the right body to do this or use Ofcom's existing role and build on that. That is a choice.

Viscount Colville of Culross: Are you prepared to put a figure on what the social levy should be? A percentage or a number?

Clare Sumner: That would be quite hard to do.

Q146 **Baroness Bonham-Carter of Yarnbury:** Picking up on two things that have already been said, I think I know what the answer to my question will be. It was interesting that Clare said that people think that YouTube is regulated, and Magnus talked about worlds colliding. We also have written evidence from Channel 4. Should online platforms be treated now in a similar manner to publishers and found to be liable legally for the content that they host?

Dan Brooke: The answer to that, broadly speaking, is undoubtedly yes. I am absolutely amazed that we are still having this debate. The fact that we are is a matter of legal weaselling—nothing more than that. Self-regulation for us would be the ideal first port of call. That is what exists by way of content standards. It is clear, however, that that system has not worked. It self-evidently has not worked.

What is the alternative? We would have to be realistic about that. Asking online platforms, and social media platforms in particular, to somehow pre-approve all content that gets uploaded to their platforms is totally unrealistic. What is realistic, however, is to ask them to scan their platforms for content that is either illegal or harmful, to identify it, take it down promptly and ensure that it is kept off the platform. That is not unreasonable. The secret filming we did in a Facebook moderation centre in Dublin clearly shows that they are not capable of doing that off their own bat on the basis of the evidence of that programme. Maybe that is a one-off but it did not seem like a one-off.

To us it is absolutely clear that a code of practice needs to be introduced, and there needs to be clear liability for what happens if that code of practice is not met. They cannot introduce it themselves so it would need to be introduced by somebody else—Parliament.

Magnus Brooke: I broadly agree with that. It is time to turn the current presumption on its head and start from the position that they are responsible for the content.

My position is slightly more nuanced however. First, you need to distinguish different types of content. Take advertising content, for example, we cannot see why an online platform ought not to be wholly responsible for the compliance of the advertising content that they carry and for the acceptability of where it is placed, just as television companies are. The truth is that their sales teams sell the advertising, they get the money, they take the advertising and they put it in the place where they want to put it. They can or could have control over that entire process. That is their content. That is not content being uploaded by individuals over which they have no control. That is one category. They ought to be responsible for that. They ought to have a duty of care. The regime ought to apply to them. At the moment, it does not.

Secondly, there is the question of the other content. Here I agree with Dan that the truth is that the sites have been adept at keeping certain forms of content—pornography, child abuse imagery and so on—off their platforms, which indicates that they can, if they put their minds to it, be pretty effective in the way that they run their platforms. Leaked documents at the weekend suggested that Google sees itself as a moderator-in-chief. So it could be done, but you need to be realistic about continuing to have a platform of open access where there is no delay in uploading content. Finding that balance is the trick.

Clare Sumner: Unsurprisingly, I agree with much of what has been said. I looked at the DCMS Select Committee report because I think that these terms are getting outdated. It was interesting that they asked why we should not start from scratch, what these organisations are for and what they are doing now. When they were first established, we saw them as distributors. They were the pipes. I read that they are actually passive aggregators. They are not doing anything passively, however.

How much they target advertising and various things to consumers is hugely managed and controlled, as Magnus has said. Equally, how some of their algorithms for service news and information are managed is also very controlled. So the question now is about harmful content, content that is wrong, and about how they establish more self-regulation that we can all have faith in, in the way other organisations have.

In order to do that, as I said earlier, they need to have a legal framework and a backstop. Otherwise, there is a danger that we keep relying on them to come up with their own codes of conduct and we find the behaviour that we are all concerned about after the horse has bolted. Probably the time has come now to look at something more formal.

Q147 **Baroness Bonham-Carter of Yarnbury:** The other thing that has come up a lot in our evidence is that everyone is now concentrating on this. You are saying that we may have been a bit behind. We tend to think about the big companies. We also have to think about the smaller companies. That may be what Magnus was addressing: that you have to have the ability to allow a certain openness but also regulation.

Magnus Brooke: Yes.

Clare Sumner: There is another thing, which is that we have got used to things coming on very quickly. Everything comes on immediately. One of the things we particularly do with our children's services is moderation, where things might come on a little more slowly. The sense that everything needs to be up immediately is perhaps sometimes not quite as true as it appears. That is how the culture has changed. We expect everything to be immediate. If that is the case, you have to have these take-down mechanisms that work quickly and self-policing communities. This leads you to education which we touched on briefly. It is critical that people are equipped to both challenge and ensure that things are taken down quickly.

The Chairman: Before we come back to Baroness Bonham-Carter, may I ask Magnus Brooke for clarification? Is it your position that online advertising is effectively unregulated?

Magnus Brooke: No, I do not take that position in the sense that the ASA does as good a job as it can in regulating online advertising. The central difficulty is that the platform itself is not the entity that is being regulated. The advertiser is being regulated, not the platform. As far as the platform is concerned, it takes an advert. It does not matter to the platform what is in the advert or where it places the advert. It is simply a concern for somebody else. It is one reason why you see bad outcomes in the incentivisation of things like fake news: because the platform does not need to worry about that. That is someone else's problem. It is the advertiser's problem. The advertiser is at one remove from the crucial decisions that are being made about where that advertising goes.

Compare and contrast broadcasters who are absolutely responsible for everything we carry. We have to make sure that the advertising complies and we put that advertising in a place that is appropriate. It is a fundamentally different system and the result is a completely imbalanced system overall, because the platforms can take an advert and literally put it up as soon as they get it. We have to go through a lengthy and extremely expensive compliance process. We spend millions of pounds a year complying adverts.

Baroness Bonham-Carter of Yarnbury: I have a supplementary question. Do you think the provisions of the e-commerce directive are still fit for purpose?

Magnus Brooke: In principle, I think they are. The difficulty is who does and does not qualify for safe harbour. It was conceived as being a bit like the Royal Mail, which is not responsible for the content of people's letters, or the telephone network, which is not responsible for what people say on the telephone. That is the original concept, but we have moved a million miles away from that with some of these platforms. They are, in effect, global media platforms competing against media providers such as the ITV, BBC and Channel 4.

What we see at the moment is increasing challenge, with endless litigation in the courts over whether those platforms are or are not caught by or protected by safe harbour, and you can see that across courts in Europe. We have a very uncertain situation at the moment where they defend this privilege case by case and you end up with an uneven playing field and uncertainty about what is or is not covered.

The other thing is that in the end you get to a point where you say: let us forget that. We need to accept that they are active players and not passive players, and we need to put a regime in place for that moment, which is probably quite close, when the courts say that they are no longer covered by the regime. You will then have chaos unless you put a regime in place to replace what we have at the moment, which is effectively no regulation.

Clare Sumner: I repeat the point I made earlier about passive and active, because that is where the e-commerce directive needs to be updated.

Dan Brooke: It was put in place 18 years ago before YouTube and Facebook existed.

Q148 **Lord Goodlad:** In your view, what principles and best practice for content moderation and the handling of complaints could be transposed from broadcasting to online?

Clare Sumner: The framework that the BBC operates, which I believe Ofcom spoke to you about, has some resonance here. We have clear editorial guidelines which set the standards for what we expect all our journalists and content makers to meet. The BBC has a particular mission and particular public purposes, so getting that content right is important for us. It starts, however, by having clear guidelines and standards which everybody as they come into the organisation is inducted and trained in.

Regarding what happens next, we have a clear policy of "broadcaster first". The complaints come into the BBC first. This is slightly updated with our new charter, but essentially, we try to answer 90% of those complaints within two weeks. If we get it wrong, we try to say quickly that we have got it wrong, and we try to explain the context if things are not as our audiences think they should be. Then there is an appeals process within the BBC and a final appeals process to Ofcom, which is the more controversial cases or the ones where people have real concerns about harm done or something like that.

One of the things that has come up in this debate is the scale of content that some of these platforms have and are operating under. How would you deal with a system like that? You probably have to begin to categorise the areas that are of real concern. It is easier for the platforms if the activity is illegal; you referred to pornography or something that encourages real harassment. That obviously has to be taken down immediately. It is about enabling consumers to have more transparent mechanisms for how they complain, who they complain to and how their comments get resolved.

It is also about whether—this is a really hard question, because it requires scale for an organisation to do this—there should be any appeal mechanism for an individual if they feel that they have not been treated appropriately, and about how you would seek to make that manageable. That is a very difficult question, but it is not one that we should duck. You either have to get that consumer accountability up front by being clear about what you are signing up to, what it means and whether you agree, and having more transparency in that, or you have to have clearer mechanisms: if this is not how you think it should be, what do you do?

Dan Brooke: The short answer to the question is that there is a lot that can be learned from broadcasting by the online world in content standards because there are very strong content standards in broadcasting and there is almost none online. I thought it would be interesting to bring to your attention some of the details that we learned from the documentary where we sent journalists to film secretly in the Facebook moderation centre in Dublin because it yielded quite a lot of information which up until that point was not in the public domain. It is worth comparing some of the things that we found to what we at Channel 4 are subject to.

Is there a dedicated UK content code for Channel 4? Yes, it is the broadcasting code. With Facebook, is there a dedicated UK code? No, there is not. There is one code that applies to the whole world. Is the code set by an independent third party? Yes, in the case of Channel 4 it is set by Ofcom. In the case of Facebook, no, it is decreed from Silicon Valley by Facebook. Is the code published? For Channel 4, yes. The Ofcom broadcasting code is published for everybody in the world to see. For Facebook, no. We had to send in hidden cameras to yield some of the information about what their content standard codes were.

Does the code apply to all content? Yes, for Channel 4 and for all the PSBs. For Facebook, no, they only look at content that has been flagged by users. What percentage is there of that content, or all harmful or illegal content, on Facebook? We have absolutely no idea because nobody knows and nobody has the full view of what is on Facebook because all of our news feeds are personalised. Are there sanctions for not following the code? For Channel 4, yes, we might be forced to make apologies or fined or ultimately lose our broadcasting licence. For Facebook there is absolutely no sanction whatsoever.

You can see that in this specific tale. It is slightly contradictory, but coming from Channel 4 I can occasionally afford to be slightly contrary to Magnus. There was a video about child abuse that featured in our documentary where there is a very unpleasant video of an adult abusing a child that was used as part of the training for the moderators in the centre in Dublin. The people being trained were told, "You have to keep a video like that up because that is a way of helping to find the perpetrator".

The perpetrator was then found. It turned out he was in Malaysia and he was arrested. The Facebook code requires that once the perpetrator has been found, the video should be taken down. That was the understanding about what had happened. It then took a session of a Select Committee in the Irish Parliament who had called Facebook in front of them to ask questions specifically about the programme that we had put out. They were asked whether the video had been taken down. They said "Yes", but in fact it had not and was then hurriedly taken down. That was weeks ago. I checked on my phone this morning and the video is back up there.

That tells us a lot about how effective are the systems they operate and what kind of impact there is around complaint and appeal. Maybe that is a one-off but it is what we found because of a specific activity. What appears to have been created is genuinely a Frankenstein's monster where the person who created it does not fully know exactly what they have created but it is lurching around knocking into people and knocking into things, perhaps unintentionally. I do not think that they are doing anything more than wandering around after Frankenstein's monster with a tin full of sticking plasters. They are dealing with whatever they need to deal with in order to stop PR problems rather than fundamentally dealing with the problems.

Magnus Brooke: I would not disagree with any of that. The critical point is that being effectively regulated, having a regulator that is capable of getting to the bottom of things, is capable of enforcing the rules and potentially penalising people who do not obey, is what concentrates the mind. In Germany, for example, where the German Government has brought in the law around take-down it is striking to see the extent of the improvements in take-downs. I read in the Commons Select Committee Report that a sixth of Facebook's moderators now work in Germany, which is also very striking. That is the answer because it concentrates the minds of commercial organisations.

Baroness Kidron: Something was troubling me a bit because you all gave fantastic explanations for why they were responsible and that they are not acting like platforms and so on, but you each in your own way said that they cannot be responsible for their content, although you did not use those exact words. I struggle with that idea and I want to put to you that if they are getting revenue from something that is popular in the example that Magnus gave, where they are putting something next to content, is there something that one should be looking at that is proportionate? Do you really believe that they are too big to have a look from the beginning at all the content because their size is reflected in their share price, which is also reflected in what they could put towards solving some of these problems? I was interested that all of you, while being very acute that they are responsible, also backed off and said that actually they are not.

Dan Brooke: They are responsible for their content. What I think is unrealistic is to ask for them to be responsible for the pre-approval of any content that gets put up. I think that is hard because it is such a vast ocean.

Clare Sumner: I struggle with it too. As I was preparing for this Committee, I read the Ofcom report which said that it is so big and so unwieldy and how do we do this. I do not think you would be able to do the whole lot. I wonder if you need clearer demarcation between community zones, such as where are people having their own conversations, clearer attribution and sourcing, particularly to information which is critical with fake news, and potentially the capability which they could afford around moderation in some of these areas.

The whole premise of how we define an open internet, which we talked about at the beginning, is critical here and whether it could be segmented. What it would mean as a consumer, because you need consumer buy-in in this conversation, is whether therefore the pace of things coming would naturally slow down. What moderation means is that you cannot do immediate posting and immediate content making in quite the same way.

The question is probably one of scale. I do not think that you can do the whole thing. Are there particular areas where it would be more advantageous for a bit of time? The other thing, which I appreciate we will be coming on to later, is how do the algorithms work that then surface content that enables people to be informed across a range of sources and not then lock down into what I would call filter bubbles or echo chambers.

Baroness Kidron: If I have understood what you are saying it is that it would be good to know if you were in a church or shopping mall or a playground and then act appropriately.

Clare Sumner: Yes. It is about naming things and being clear with consumers about what this relationship means. For example, I give my personal data to Facebook. I appreciate that in my feed I get information about slippers or sportswear or whatever. I take that as the consumer relationship that I have and I am getting a service back for free. The other thing we have not talked about is they are highly commercial operators with advertising but the deal with the consumer, which is why in part many of us sign up, is because they are giving us something that we find useful. There is that community sense, bringing people together and sharing information. The question becomes that when you are looking at more things that we would almost call broadcast material in this country—news, drama, videos and content—should there be something around that which we could segment more clearly? I agree that the sheer scale of it means that if you try to start with all of it, it is all a bit baffling. You have to segment it.

Magnus Brooke: I would distinguish between the advertising because I think the advertising is key. They can and should control where their advertising goes. To the extent that they are putting advertising around content, they ought to know what that content is and not put it around inappropriate content. That seems to be relatively straightforward. It is harder when you have content uploaded over which they do not have visibility or control at all times. You can reverse the presumption, however, and say that we are going to hold you responsible for the content as the starting principle but we are going to carve out or find ways to make that possible. We will then pass the responsibility to the regulator with the most serious harms in mind for it to figure out what the best efforts look like.

For instance, how much should you be spending? What should you be doing in order to get as close as you possibly can to preventing harm without necessarily being entirely responsible for all the content at all times because you would struggle to do that? Part of the role of the regulator is to say, "These are the harms you want to prevent and this is what best efforts look like. This is what we expect you to do in terms of moderation, in terms of use of algorithms, in terms of the harms that we are seeking to prevent", in addition to the control over advertising. You may not get all the way there but you will get quite a lot further than you are at the moment. That is at least a starting point.

The Lord Bishop of Chelmsford: Magnus started to answer my cracked-record question that I keep asking about pre-approval. I do not see why there could not be a much greater degree of pre-approval and you could turn the moderation thing on its head. Rather than moderate about the content that should be taken down, you moderate the other way over the content that is being prevented where you say, "No, could you please put it up". Some people would say that that is censorship. I do not see why that should be the case. If the moderation works then the content is put up; it is just delayed a little. Why can you not turn it all on its head and why can the clever algorithms which are so good at selling me slippers and sportswear and clerical garb not do this work?

Dan Brooke: That would have to be through artificial intelligence. I do not think there is any other way. Despite their vast wealth, the idea of doing that exclusively via human beings seems unrealistic. I am no advocate for the social media platforms, as you can probably gather, but there is the sheer vast amount of content. That does not mean that I think that, given all of the content, the proportion of it that might be illegal or harmful could not be weeded out. That part is and I think it is possible to do it properly. The evidence that exists thus far and what we know about in Germany shows that.

To build on what Magnus was saying about the German example. We are particularly exercised about fake news. Facebook is where the issue of fake news is strongest. Facebook have said and trumpeted strongly when

Zuckerberg gave evidence to Congress that they have doubled the number of moderators from 10,000 to 20,000 people, which sounds terribly impressive. They are the people who are responsible for safety and security. It turns out, however, that we do not know what safety and security means. It could be people who are trying to hack Facebook's website or it could be the physical security for their offices around the world. It transpires in the same evidence to the Irish Select Committee that 7,500 of them were moderators. If there are 7,500 moderators, and if one in six of them is in Germany, that is 1,250 moderators covering content in Germany. What did our programme find? The number of people on the ground in Dublin dealing with UK content was about 12 at any one time. Germany has strong regulation and that is motivating Facebook to put on the ground 100 times more content moderators than it appears are dealing with UK content.

There are other differences between the UK and Germany but the population sizes are not vastly different and the cultural differences are not vast. What is it that is motivating them to make that big change? Clearly it is regulation and that suggests to me that they believe, from their viewpoint of understanding the entirety of their platform, that content moderation is the absolute key to keeping it cleaner.

Viscount Colville of Culross: May I ask a supplementary to that? You praised the German example. Many people have said that the German law has been counterproductive and acts as a control on free speech. It has made heroes of the AfD, the far right. Is there not a concern that if you put as much energy into it as the Germans that the upside is they have lots of content moderators and the downside is that they seem to take down an awful lot more than they should, certainly if you want free speech.

Dan Brooke: No system is perfect. I would look at the British system for the regulation of television news. What we do rests, particularly in Channel 4, on being able to fulfil the concept of liberal free speech that we have in this society. Yet we also have the strictest form of regulation around television news and the by-product of that is that we are still people's number one source of television news and we are also the most trusted. There are lots of imperfections and the system and I am sure it can be improved, but it shows me that the concepts of free speech and regulation can co-exist successfully, if not perfectly.

Q149 **Viscount Colville of Culross:** To declare an interest, I am a series producer making content for the Smithsonian Institution digital channel and for CNN. I want to bring up the issue of the cancer of fake news, as you call it. Our sister Committee, the DCMS Committee in the House of Commons, when looking at this subject called for the Government to do proactive work to introduce transparency in this area. Facebook has come back very recently saying that it has introduced transparency in sourcing and where the user is or where it lands. It is also, so BBC evidence tells me, advising people to sign up to the fact-checking code of principles. Is that enough? What more needs to be done to force or introduce transparency into the social media platforms in order to counteract fake news?

Clare Sumner: The BBC’s view on this is that it is our public purpose number one to provide independent and impartial news. In an online environment we work very hard to give our audiences a mix of sources where they can check information. One that you may have all used is Reality Check where we broadcast information to, but primarily on the web you can look up and see if you want to find out more about exactly what a hard border means. The other thing to bear in mind, particularly with younger audiences, is that they are coming to the BBC as the place where they check facts and information, which is very important.

To answer your question, I would like platforms to do more of ensuring that when you are in those streams you can easily see which stories are from which organisations, particularly PSBs, and begin to think about not a legal framework solution but a practical one. Particularly in this country, and not just the PSBs but our newspaper industry as well, we have clear regulation and clear principles about the way we operate. Perhaps it could be easier to come out of the filter bubble and link in to other sources. If you think about BBC Online, you can link to other newspaper sites or online sites to get more information about what you are looking at. That sort of approach is important. Some sites have begun to source recognised contributors so that you can check the credibility of who is making comments and giving information. That is important because in order to protect freedom of expression we need to understand where each of us is coming from. If you represent a particular point of view, I as a consumer can see that easily rather than be forced to not quite be able to work it out.

Viscount Colville of Culross: Should we legislate in order for that to happen?

Clare Sumner: That is a good question. At the moment we have a halfway house. On the prominence debate, there is something interesting in the news space in that perhaps we should be looking more at how we link out to a range of different sources. Coming back to Lord Gordon’s point earlier, the specificity of that may be too much in terms of detail but at a principle level the fact that in this country consumers should be able to access a range of news sources is something that we should perhaps be looking at more. That would be my attempt at trying to do something like that.

Magnus Brooke: There is quite a neat link here to the Cairncross review looking at the future of news. You can see a sort of sweet spot solution coming out of that as well as out of the TV prominence debate that we have been working on which all goes to the same basic point. You have global platforms seeking to shape the worlds of British citizens and British consumers. As a Parliament, do you want to do some things as a result of which British news and news from credible organisations that submit themselves to regulation or are in other ways verified, would get some priority in the lists and in the news results that are surfaced? It is not just about television; it is about the press as well.

On the commercial incentivisation point, I am sorry to bang on about this again, but there is some simple stuff you can do to start with. Quite a lot of people are creating fake news to make money. There are of course state actors seeking to create fake news for different reasons but there an awful lot of them doing it to make money. We can start by making sure that they do not make money out of fake news. That can easily be the responsibility of the platform because they just have to do their homework about where they are putting their advertising. All of these other solutions are more difficult, more complicated, will take more time and will probably require some form of legislation. All go to a similar point, however, which is: what has surfaced, how prominent is it and how much do people use it and pass it on?

Dan Brooke: If I have understood your question correctly, a lot of those things are contained within the concept of self-regulation which has been shown to be completely wanting. The only way of dealing with that is for an independent third party to impose a code of practice and to ensure that there is liability if those codes of practice are not met. It is up to the platforms to figure out the best way of policing their own platforms to ensure that this or that type of content that the code requires should not to be on their site. I would observe that in the many things that we are told, such as "We are trying this or trying that", there is still an enormous amount of opacity about what those things are and what impact they have.

The biggest thing that appears to have been done differently, which has come from piecing together, as I did a second ago, information around how many moderators they have around the world, how many are in Germany and how that compares to the UK and so on, is to add a significant number of moderators. That suggests to me—suggests, because I do not know—that the best way to combat fake news is probably an element of artificial intelligence and to have human beings moderating content. The more people you have doing it the quicker that is going to occur. We all know that part of the problem is that a lie can get halfway around the world, as Churchill said before the internet was even invented, before the truth has got its boots on.

Q150 **Baroness Kidron:** I want to ask you a little more about algorithms, which have been cropping up here and there. In a conversation I had the other day someone, who is a leading thinker on this, said rather brilliantly that the biggest failure of algorithms is that they have been over-marketed. They do not work as well as we think. We have a problem in that they do not work very well. It may be that they work too well in certain environments, but we are not sure what working well looks like. Can you each say something about that? I was going to ask you, Clare, if you could particularly mention the piece of your evidence which said that the BBC thinks that data should belong to the user but, in the meantime you will be using it. I was quite interested in that nuanced approach.

Clare Sumner: On the broader question, the BBC is asking people to sign into our services and become registered users so that we can use the data to make personalised recommendations about the content that we manage. This is not commercial in any way. It is trying to surface the programmes that you like and enjoy already and it is also trying to think about the serendipity of inform, educate and entertain that we can create on a linear schedule that in a digital environment is sometimes more difficult. When we look at data, to answer your specific question, that is what we are trying to achieve with it. If any of you are signed-in as registered users you will have emails saying, "Have you seen this programme and have you also thought about these things?" to try to make some connections between the content you might expect to see and some of the content we think might surprise you and that you would enjoy.

Baroness Kidron: What is your duty to us about understanding what decisions you are making?

Clare Sumner: Everything around algorithms needs to be more transparent and people need to be more honest about whether they are using algorithms and what they are doing. For example, in the platforms it is sometimes surfacing news stories and how that priority works. You will see, for example, on our BBC website that you have the running list of the stories that we think are the most important—the editorial judgment—but we also have a section where you can go to the most read. This is being clear about where they are being used so that you as the consumer can see and understand it without getting into the algorithmic equation that might be powering the machine behind it.

Dan Brooke: The openness about data and algorithms and how they are used is essential. As a public service broadcaster, like the BBC we ask everybody to give their details to use our online service, All 4, and we collect that data and use it to personalise services and target advertising better. We have something called Our Viewer Promise where we very clearly lay out in plain English, "This is what we are collecting from you, this is why we are collecting it, and this is how it is going to be used". We have won awards for that. I think that everybody should do that. It is more complicated if you are running a global social media platform but we would agree with the DCMS Select Committee that just as financial accounts can be audited and scrutinised so algorithms should be to some extent. Precisely what the limits are to that I am not expert enough to know but there is so much opacity at the moment. Anything that yields a bit more transparency for citizens would definitely be a good thing.

Magnus Brooke: I agree with that. One of the things we do is to give people a choice of a gold, silver or bronze targeted advertising service. Bronze is not targeted and gold is very targeted and we use third party information. It is clear to the user which one you are opting for. Some people do opt to get more targeted advertising because they do want to get served adverts that are appropriate for them. I agree with Dan and Clare, however, that it is all about transparency, making it easy to make your initial decision, to make subsequent decisions, but also to change your mind and go down a different route if you prefer, having had the experience.

Baroness Kidron: Can I ask whether any of you offer the user the opportunity of de-personalising them? Once we change our mind about whether we are interested in cooking or cars, can we clear our content cookies? I do not mean so much for advertising.

Dan Brooke: We have a nuclear button where you can say, "Get me out of here". The promise is that all of your data is deleted and it is deleted.

Clare Sumner: I think we have something similar but I will check. The other thing we have is the ability to keep updating what your interests are because they might change over time. I might be into natural history this week and into something else next week. I will double-check on that point.

Q151 **The Lord Bishop of Chelmsford:** I want to ask about safety or Secured by Design. The background to this is research the BBC has done which shows that about two-thirds of 10 to 12-year-olds have a social media account yet, as we know, most social media platforms have a minimum age of 13. We are aware that some of the BBC apps have good parental controls and guidance. The question for all three of you is how you incorporate Secured by Design into your products and services? What advice can you give us about how such principles might be enforced or promoted, although I think you are probably going to say enforced?

Clare Sumner: You are right in the question; it is how they are designed in from the start. For example, we have something called CBBC Buzz for under-13s. You have to verify your age and get parental consent. This is an idea for sharing creativity and games in our programmes. It is a moderated site. You can keep some stuff to yourself if you do not want to share it, but if you do want to share, it goes through a moderation process. I would say that, particularly around children which is a very specific area if you are looking at children's content, this could be looked at. The Government have started to focus on children as well. There is something about the design and transparency, accountability and being clear about the parental controls. The old watersheds were put there for a reason. Making sure that within a digital environment there are parental locks that you can apply and content signs similar to film classification about what are we watching are all relevant.

The other important check on this, as a colleague reminded us a few weeks ago, is the role you have as a parent, and I speak as a parent, in ensuring that you know broadly what your child is up to in this space. There is something about ensuring that parents know what is available to them. Coming back to education on online interactivity, the BBC has done a lot to promote that and is going to do more. We are looking at wellness apps and things like that so that we use technology in a good way and recognise where it can become too addictive or you end up using it too much. Some of that is an important parental responsibility as well. I do not want to sound too preachy but it is important.

Magnus Brooke: I agree with all of that. There are a couple of points I would make. One is about the content. We control all of the content on our sites. It is a walled garden fundamentally and it consists of content all of which has been made to standards that are appropriate for linear television. One of the things you know about contemporary childhood is that the one place where parents are happy to put their children is in front of linear television. It is a safe place compared to online. The second is PIN control. Like the BBC, we offer parents the ability to PIN control content on our sites. We offer visible guidance warnings with explanations about why particular content may or may not be suitable. There is a range of things. There does, however, need to be a degree of education of parents that more is expected of them online, even on services like ours, than is expected on linear television because you are giving people more choice, you are trying to give more tools to parents and there is a degree of responsibility there as well.

Lord Gordon of Strathblane: On the issue of prominence, we have moved from linear broadcasting and are in the process of online streaming et cetera. How are you going to manage this, bearing in mind that there may be a legitimate conflict between what people want as consumers—and online providers can provide them with what they want—and what they ought to have as citizens which public service broadcasters want to give them? How are you going to square that circle?

Magnus Brooke: At the moment at least I am not sure there is that much of a circle to square. The truth is that the services we provide are incredibly popular. The consumption levels of PSB very high.

Lord Gordon of Strathblane: So you are not worried by Sky directing viewers with their Q control "to programmes we know you like"?

Magnus Brooke: That is exactly what we are worried about. We are worried about global platforms who have global incentives to favour their own content or to favour content of their partners which they put in more prominent positions to try to change the muscle memory of the audience when actually from the audience's point of view a lot of the time what they are trying to find is PSB content. The problem is one where the incentives of global operators are different from the incentives and interests of UK consumers. We are saying that UK consumers do want to consume public service broadcasting content at scale. Even though they have had in the UK for many decades a huge amount of choice, the PSB services are still immensely popular. We are worried about attempts to try to effectively hide PSB content so that it is harder to find and eventually people just give up and say, "I cannot find this stuff and it is not easy to access. I will just settle for this other content". In our experience, it is not what they want but it may be what happens because PSB content gradually drifts further and further away from the screens that people see easily when they turn their devices on.

Lord Gordon of Strathblane: How can this be prevented?

Magnus Brooke: There are a number of ways we can do that. The critical thing, as Clare said earlier, is not to set a prescriptive framework in primary legislation. At the moment we have the EPG rules. The EPG rules have worked because effectively EPGs have not changed for 20-odd years. It has been a fairly static method of accessing television. The problem that you are going to have over the next 20 years is that accessing television is not going to be static in any way at all. What you have to try and do is establish a primary legislative framework which says that these services matter to us and that we want them to have a prominent position on interfaces which people use in large numbers to access television services.

Baroness Bertin: I hear what you say and have huge sympathy about prominence rules and regulations. You made the point about sticking plasters in a different context. The size of their pockets is huge, so I am curious to know how seriously you are taking that. We do not have much time but it strikes me that changing the rules around prominence will not be the answer.

Magnus Brooke: If it were far reaching enough it could make a big difference. If you look at the effort that, for example, Netflix is making to secure prominence globally on screens that open when you turn your device on but, even more importantly, on remote controls, it gives you a feel for the extent to which people are fighting for the public's attention in the living room. We are saying that you can do something from the legislative point of view to say that the services we value ought to be in the prominent positions that Netflix will seek to buy and you are setting yourself up in the UK with a system where you have the best of all worlds. You have got Netflix, of course. We all consume Netflix as it is a terrific service but alongside it we do not want five other Netflix, we also want to have the PSB services.

Clare Sumner: We are trying to ensure that UK consumers have a choice when they get to that interface. The old interface was the linear channel with one, two, three and four. That has moved on a great deal and what we are saying now is that it is beyond our linear services, it is to our online services. When you look at the prominence of those on UIs there should be equality in that so that the consumer makes the choice. Coming back to what our audiences want, at the moment they rate all of our services very highly. Why do they rate them so highly when we cannot compete with "The Crown" of Netflix which cost millions of pounds? The BBC's response is that we have done 18 series of UK dramas that reflect our society in a way that resonates with our audiences both young and old or particular parts of content such as "Blue Planet II", which is genuinely ground-breaking and global.

Part of it is that some of the responsibility is on us to make really good content that everybody wants to watch but another part of it is about the recognition of what our brands respectively mean and what we will be investing our much more limited resources in. Netflix spends $8 billion. We as PSBs spend £2.5 billion on drama. That is a huge differential. We have got to make sure that that investment in British content and British talent really counts. To our credit, there is some great content going on at the moment. You are hopefully enjoying some of it, whether it was "Bodyguard" or "Killing Eve" or "Wanderlust". There are some really amazing pieces on at the moment and that is what draws our audiences in. Our fear is that in the current system there is a danger that Netflix can pay for the remote-control buttons, that commercial decisions are made about which thing goes here linked to advertising which would diminish the availability of content that the British public have said that they like and contribute to, in our case with the licence fee. That is really valuable in terms of the overall service that we provide. That is why I also mention news in this debate. The attribution and sourcing of news is really important and it goes together.

Dan Brooke: I do not think that we would say that prominence is the be-all and end-all answer to the future health of the public service system but it is a significant one. In the quid pro quo that is the PSB system, let us ask broadcasters to make a whole load of content that is good for society and good for citizens but we think the market might not otherwise provide and let us make that prominently available. That also helps the audiences of the providers which allows them to be well funded to ensure that there is a strong business model for the production of that content. That is a principle and a logic flow which has existed for decades. That does not mean that it still has a place today and should be examined, but there is a set of principles there that Parliament and industry have bought into. Although it does require legislation, it is not a reinvention of the wheel. We are talking more about a re-treading of the tyres and updating a system that already makes a lot of sense for the modern age because the way that people watch television has changed and therefore the system should change. We believe that it will make a difference, otherwise we would not be going on about it so much.

Viscount Colville of Culross: The Government have said that it is nonsense.

The Chairman: We will write to you so that you can get on the record on the issue of copyright in particular which we would like to explore. I thank our witnesses for their evidence session today which was very useful. We may well be in touch but with five minutes before our deadline I will suspend the session. Thank you.

BBC – supplementary written evidence (IRN0119)

Follow-up responses for House of Lords Communications Committee

Question 9

What assessment have you made of the revision of the Audiovisual Media Services Directive insofar as it affects the regulation of TV-like content?

While it doesn't affect the BBC directly, we welcome the revised Directive. It's good for audiences as it aims to create a more level playing field between traditional broadcasters and video on-demand services.

The revision aims to do two things. Firstly, to improve protection for children using video on-demand services. Secondly, to increase the contribution VOD services make to audio-visual production in Europe by requiring at least 30% of their catalogue to be made up of European programmes.

As the Committee knows, the BBC and other UK public services broadcasters already deliver the highest standards in child protection and a very large proportion of UK programming. That means the revision does not affect us directly. However, we think it's good for audiences for the editorial standards between traditional channels and VOD services to be brought into line, particularly on important issues such as protecting children online.

Question 11

a) *Article 13 of the Copyright in the Digital Single Market Directive will place specific technological requirements for platforms. Is this the right model in your opinion?*

b) *Who should bear the costs of developing and managing these systems? The platforms or the copyright holders?*

The BBC does not have a view on 11a).

As a rights holder and rights user, the BBC believes platforms should act quickly and transparently to remove copyright infringements and ensure they stay down. It is important that this applies to all platforms, as it will not be sustainable if some platforms benefit economically from copyright infringements while others are investing in tackling it. An effective copyright regime is vital for the strength of our world-leading creative industries and the quality and choice we offer audiences.

Question 12

a) *What are the risks if the UK introduces regulation without the co-operation of international partners, particularly the European Union?*

b) *What other international bodies should the UK work through to improve internet regulation?*

The UK has long been a global leader on policy and regulation. For example, the UK Government, Ofcom and industry's work on net neutrality became the core of the EU's regulation in this area.

We welcome the Culture Secretary's and Ofcom's recent comments on the importance of the UK continuing to play a leading role in international regulatory debates. The BBC can also play its part. For example, Tony Hall was recently elected incoming President of the European Broadcasting Union, a body which plays an important role in furthering gold-standard public service broadcasting.

There are risks if the UK seeks to introduce internet regulation without international collaboration. Foreign states could attempt to misrepresent efforts to address internet harms in the UK as the equivalent of attempts to stifle freedom of expression in theirs. The BBC's website, for example, continues to be blocked to all but a few elites in DPRK and those using VPNs in China. As the UK seeks to devise rules for the internet, it should do so in an open, transparent and globally collaborative way.

Supplementary Question - sign-in and personalisation

The Committee asked during the oral evidence session whether it's possible for audiences to 'opt-out' of personalisation on the BBC.

I am pleased to confirm to the Committee that all users have the option of opting-out by turning off 'Allow personalisation' in their account settings. Users who opt out of personalisation will, for example, not get personal recommendations based on the things they've watched and will receive generic versions of the newsletters they have signed up to.

The reason we ask people to sign in to access content online, such as BBC iPlayer and BBC Sounds, is because it enables us to make personalised recommendations, tailor services such as local news, sport and weather, and remember how much of a programme users have watched. It's really important that we're transparent about how we use data to personalise our services. Audiences can read about why we collect data, how it is stored and how they can opt-out at www.bbc.co.uk/usingthebbc.

20 November 2018

BBFC – written evidence (IRN0068)

Executive Summary

- The BBFC's role is to protect children and other vulnerable groups from harm and to empower consumers, particularly families, through classification, content information and education. It operates transparent, trusted regulation based on years of expertise and published Classification Guidelines. Since 2008, it has been working in partnership with industry to bring, as far as possible, offline regulatory protections and guidance online. For example, the BBFC is the independent regulator of content delivered via the UK's mobile network operators - content that would be age rated 18 or R18 by the BBFC is voluntarily placed behind filters for those under 18 on all non-age verified devices.
- The BBFC welcomed the UK Government's Internet Safety Strategy Green Paper and Digital Charter because we share the ambition to make Britain the safest place in the world to be online and to ensure that what is unacceptable offline should be unacceptable online. There are various models of effective regulation, ranging from self-regulation using trusted standards to a statutory framework.
- The purpose of age ratings and content advice attached to film, TV and video online is to protect children and enable consumers to make informed viewing decisions. There is a strong case for consistent age ratings regardless of how content is consumed by the UK public. Research shows that 85% of UK parents want consistent age ratings in cinemas, on DVD and online (Bernice Hardie, 2015).
- The BBFC recognises the importance of appeals mechanisms, even where regulation operates on a voluntary basis. The BBFC therefore provides an appeals service to respond in a transparent and timely way to reported cases of over and under blocking by access controls and filters on mobile devices.
- Entry into force, by the end of 2018, of Part 3 of the Digital Economy Act (DEA) 2017 will protect under-18s from pornographic content online through age-verification controls and by preventing access to 'extreme pornography'. The Government designated the BBFC as the age-verification regulator because of its demonstrable expertise in pornography and regulation online. The BBFC believes that this new regulation of online commercial pornographic services will be a significant child protection measure and will set an international precedent.
- The BBFC and the Dutch regulator, NICAM, developed a tool - You Rate It - that enables crowd-sourced, bespoke national age ratings and content advice for user-generated content (UGC) and includes a report abuse function. Following a successful pilot project with the Italian media company Mediaset, the BBFC believes You Rate It should be tested further in the UK/Europe in partnership with industry.
- The concept of age rating online music videos is accepted by all three UK major record labels, along with Vevo and YouTube. But this initiative would be more effective if international repertoire were brought into scope.

Currently some of the most controversial music videos are not being regulated. In addition, there could be more prominent age ratings on platforms, ideally tied to parental controls.

- The BBFC supports regulatory initiatives to make the internet a safer place, with a particular focus on protecting children from inappropriate material online. The BBFC's experience is that consumers expect protections offline to be replicated online. The BBFC would urge the Lords Communications Committee to consider further the value of trusted systems for labeling of content, which reflect national sensitivities and which can be linked to filters and parental controls. We believe that the BBFC system of classification meets the key criteria for child safety online. Namely, having:

  - child protection at the core;
  - effective labelling of content so that standards are trusted and understood, because they reflect national sensitivities, and the symbols used are recognisable;
  - broad coverage so that the system creates a known standard;
  - low cost; efficient, flexible and innovative service so that it can keep pace with technological change and not be burdensome on industry.

1. Introduction

1.1 The BBFC is the independent regulator of film and video in the United Kingdom. Since 2013, the BBFC has been the independent regulator of content delivered via the UK's four mobile networks (EE, O2, Three and Vodafone). The BBFC was also designated the age-verification regulator under Part 3 of the Digital Economy Act (DEA) in February 2018.

1.2 The BBFC operates a transparent, trusted classification regime based on years of expertise and published Classification Guidelines. The BBFC conducts regular large scale public consultations to ensure that the standards enshrined in its Guidelines reflect public opinion. The BBFC's primary aim is to protect children and other vulnerable groups from harm through classification decisions which are legally enforceable and to empower consumers, particularly parents and children, through content information and education, enabling families in particular to choose content well, wherever, whenever and however they view it.

1.3 The BBFC is a member of the UKCCIS Executive Board and participates in a number of UKCCIS working groups. In addition, the BBFC works with UK and international partners, including the European Commission, on projects to improve the protection of children from potentially harmful media content online and to enable children and parents to make informed online choices.

2. BBFC Classification Guidelines – based on consultation and robust research

2.1 The BBFC classifies films, videos and websites according to the standards set out in its Classification Guidelines. Age ratings range from 'U' for Universal to 'R18'. The Classification Guidelines are the principles and standards that underpin the BBFC's general work and classification decisions, and help the BBFC to remain in step with public opinion on a range of issues in media content. Research demonstrates that the public agrees with the BBFC's classification decisions more than 90% of the time (*Bernice Hardie and Goldstone Perl, 2013*). The 2013 Guidelines consultation found that most respondents, including 84% of parents with children aged 6-15, consider that the BBFC is effective at using classification to protect children from unsuitable content. 89% of parents (and 76% of teenagers) rate classification as important, and 95% of parents with children under 15 usually check the BBFC classification.

2.2 The BBFC is currently engaged in its fifth large-scale consultation with a view to updating its Classification Guidelines. As with previous Guidelines consultations, 10,000 members of the UK public will be consulted on their views and viewing habits, including perceptions of depictions of sexual violence and discrimination, the means of accessing content online and the value of age ratings and classification when choosing what to view. The consultation involves both qualitative and quantitative research, involving adults and teenagers across the UK. The BBFC expects to publish the new set of Guidelines in early 2019.

2.3 To inform both policy and individual classification decisions, the BBFC takes an evidence based approach. We will, where appropriate, draw on expert advice in areas such as depictions of mental health in the media. For example, the BBFC maintains close relations with the Samaritans and other suicide prevention experts in relation to classification policy on issues relating to suicide and self harm. To inform classification policy, the BBFC commissions research into specific issues. Recent examples include the acceptability of depictions of sexual, sexualised and sadistic violence in film and video; and of 'glamour' content accessed via mobile devices.

3. Is there a need to regulate the internet?

3.1 The BBFC welcomed the UK Government's Internet Safety Strategy Green Paper and Digital Charter because we share the ambition to make Britain the safest place in the world to be online and to work towards ensuring that what is unacceptable offline should be unacceptable online. The BBFC also recognises that there are various models of regulation that can be effective, ranging from self-regulation using trusted standards, to a statutory framework.

BBFC Online regulatory role

3.2 The purpose of age ratings and content advice attached to long form film, TV and video online is to protect children and empower consumers, enabling families in particular to make informed and safe viewing decisions. The BBFC is committed to helping families choose well, wherever, whenever and however they view content.

3.3 There is a strong public policy case for consistency of age ratings for film and video content regardless of how it is consumed by the UK public. This belief is supported by our most recent independent research that demonstrates that 85% of UK parents want to see the same consistent age ratings used in cinemas, on DVD and online (Bernice Hardie, 2015).

3.4 Since 2008, the BBFC has therefore been working in partnership with the home entertainment industry and others to bring, as far as possible, offline regulatory protections online. In doing so, it uses a number of best practice, voluntary self-regulatory models that apply trusted BBFC standards in ways that best fit the business practices of different providers and the requirements of their consumers, particularly families. The BBFC's industry partners in the online space include:

- content providers from the home entertainment industry, music industry and adult industry
- online platforms such as iTunes, Netflix and YouTube
- access providers, including all the UK's mobile networks

3.5 These models involve the BBFC setting content standards and classifying material. Those standards and/or individual classifications are given effect to in one or more of the following ways:

- signposts for consumers, including age ratings and content advice
- parental controls linked to age ratings or standards
- internet filters
- age-verification systems

3.6 None of the above models offer a panacea, either individually or collectively. However, they do make a substantial contribution to online child safety and consumer empowerment, and have been welcomed by parents in particular. The BBFC believes its commercial partners should be recognised for the way in which they have engaged with ratings and content advice in order to protect children. In terms of how these systems could be improved to ensure parents are better informed, the BBFC has argued for a more consistent and systematic approach across different media.

4. Regulation of content delivered by mobile networks and appeals mechanism for over and under blocking

4.1 The BBFC is the independent regulator, on a voluntary, best-practice basis, of content delivered via the UK's four mobile networks (EE, O2, Three and Vodafone). Using the standards in the BBFC's Classification Guidelines, content which would be age rated 18 or R18 by the BBFC is placed behind access controls and internet filters to restrict access to that content by those under 18 on all non-age verified devices on the UK's mobile networks. This content includes, for example, pornography and other adult sexual content, pro-Ana (anorexia nervosa) websites and content which promotes or glorifies discrimination or real life violence. Customers may only remove the network filters on mobile devices if they are able to prove (using robust age verification methods, such as credit card or in-person verification) that they are aged 18 or over.

4.2 In 2015, the BBFC and EE also adopted a Classification Framework for EE's "Strict" parental setting, aimed at younger children, with filtering standards set at the BBFC's PG level.

4.3 The BBFC recognises the importance of appeals mechanisms, even where regulation operates on a voluntary basis. The BBFC therefore provides an appeals service to respond in a transparent and timely way to reported cases of over and under blocking by access controls and filters on mobile devices.

4.4 The two tier appeals procedure is open to any website owner, content provider, consumer or any other person who has an interest in the material, who is dissatisfied with the application of the Classification Framework given by the BBFC in respect of a piece of content. In the first instance, the appellant contacts the appropriate Mobile Operator, which will consider the issue. This process takes no more than five working days. If this first stage does not resolve the issue, the appellant may then contact the BBFC for an adjudication. Although the appeal is limited as to whether or not a piece of content should be behind access controls or internet filters, the BBFC may advise, if appropriate, on:

- how the content may be changed to remove the necessity for access controls or internet filters;
- whether in the view of the BBFC the content, or part of it, is potentially illegal under UK law.

4.5 On receipt of a valid written appeal request, the BBFC will ensure that the relevant website or commercial content is viewed by the BBFC Mobile Content Appeals Committee, made up of senior members of the BBFC. The BBFC will consider any written representations made by the appellant or any other interested party. The BBFC will communicate the outcome of the appeal to the appellant, the Mobile Operator and such other interested parties as the BBFC considers appropriate within five working days, provided there is no need to seek views from legal and / or other external advisers, in which case such views will be sought and considered as soon as is reasonably practicable. Stage Two appeal decisions are final.

4.6 In 2017, the BBFC adjudicated in relation to twenty one cases on whether filters had been appropriately applied to websites. These requests came from website owners, members of the public and the Mobile Network Operators themselves. In the interest of transparency, the BBFC publishes all its adjudications, in full, every quarter.

4.7 Among requests in 2017 for adjudication relating to sites that had been restricted to adults only by the mobile networks were a website offering CBD (Cannabidiol) oil/balm products for sale as a food supplement; a lifestyle website containing references to sexually transmitted diseases in the context of promoting sexual health awareness; a website offering business consultancy services; a website offering optical components for target and hunting firearms; a website offering a service providing training and consultancy for organisations to improve accessibility to LGBT customers, employees and communities; and two websites dedicated to videogame franchises. In all these cases, we found no content that we determined to be suitable for adults only. The MNOs consequently removed filters from these sites.

4.8 The BBFC also found that some sites were correctly placed behind adult filters, for example a website that promoted the cultivation of cannabis and offered instructions and equipment for its cultivation. The MNOs maintained filters on these sites.

4.9 In two cases, we were asked to consider whether websites without filters contained material that should be restricted to those aged 18 or over. The first adjudication related to two websites that contained images of a pornographic nature which we considered unsuitable for children. The MNOs consequently added filters to these sites. The second adjudication related to a website explaining the terms of use of a particular app service. The BBFC considered that this website contained no material unsuitable for children according to the Classification Framework.

4.10 The BBFC also considered the twenty one adjudications under the EE's 'Strict' Classification Framework. We considered eleven unsuitable for children under the age of 12. Such material included drug references, suggestive images and sex references, strong language, violence and gore. EE consequently maintained or imposed filters on the eleven sites.

5. Regulation of commercial pornographic services online

5.1 The literature review published alongside the Internet Strategy Green Paper '**Children's online activities, risks and safety: A literature review'** by Professor Sonia Livingstone, Professor Julia Davidson, Chair of the Evidence Group and Dr Joanne Bryce, on behalf of the UK's Council for Child Internet Safety (UKCCIS) Evidence Group examined research into the impact of pornography on children. The review found that:

- *"Exposure to pornography has adverse effects on children and young people's sexual beliefs*
- *There is evidence that extreme porn may be associated with sexually deviant/coercive behaviour*
- *Pornography is the top content-related concern for children."*

5.2 Other key research supports the case for intervention to prevent children accessing or stumbling across pornography online. In particular:

- In a survey for Parent Zone in September 2015, nearly two-thirds of parents (63%) thought that the internet meant that children were exposed to sex too early
- 60% of young people were 14 years-old or younger when they first saw porn online—although 62% said they first saw it when they weren't expecting to, or because they were shown it by someone else (BBC Porn: what's the harm? survey April 2014, conducted by ICM in consultation with Dr Miranda Horvath and Dr Maddy Coy.)
- 75% of girls aged 13–21 agree all pornography websites should have age verification controls (Girls' Attitudes Survey, 2016 Girlguiding)

Existing regulatory regime for pornographic content

5.3 The BBFC classifies all pornographic content released in physical formats, refusing to classify or removing any material from pornographic works which is potentially harmful or otherwise illegal, including so-called "rape porn". The BBFC has unrivalled expertise in classifying pornography. Indeed, it is the only UK regulator that offers a definitive classification of pornographic content. So for example:

- Ofcom uses the BBFC's classification of pornography for UK-hosted TV-like services regulated by Ofcom under the Communications Act 2003
- the BBFC is responsible for the classification of pornographic content found in video games that are otherwise regulated according to PEGI rules
- Friendly filters for public WiFi (administered by RDI) use the BBFC's detailed definition and description of pornography

5.4 The regulation, by the BBFC, of pornography offline is well-established and largely effective, including, where necessary, through enforcement measures. Online the situation is quite different. The BBFC works with a small number of adult providers in the online space on a best practice, voluntary basis, to ensure that the pornography they supply meets UK standards of acceptability and that its content is kept away from children. But in most cases, pornography is one click away for most UK children.

Part 3, Digital Economy Act 2017 - New regime for regulation of online commercial pornographic services

5. 5 The work described above covers only a small proportion of pornographic content that is accessed in the UK. It is for this reason, that the Government proposed the requirements in Part 3 of the Digital Economy Act (DEA) 2017 for the regulation of online pornography provided on a commercial basis.

5.6 Under the terms of the DEA, commercial pornographic content will need to be placed behind robust age-verification barriers in a way that secures that the material is not normally accessible to under 18s. The aim of the legislation is to protect children from harmful pornographic content online through age-verification controls and by preventing access to 'extreme pornography' under the terms of the Criminal Justice and Immigration Act 2008. The BBFC believes that this new law will substantially reduce the risk of children accessing or stumbling across pornography. It is therefore a significant child protection measure and is a key component of the Government's wider internet safety strategy.

5.7 In 2018 the Government secured parliamentary approval for the designation of the BBFC as the age-verification regulator because of its demonstrable expertise in pornography and regulation online. The BBFC was formally designated as the age-verification regulator on 21 February. In March, BBFC launched a consultation on draft Guidance on Age-Verification Arrangements and Guidance for Ancillary Service Providers. The BBFC will shortly publish a Response to that consultation and send amended Guidance to the Government. The final Guidance will be laid in Parliament for approval. The Government has indicated that the new regime will enter into force before the end of 2018.

5.8 In 2017, in preparation for the proposed new role, we actively engaged with the adult (pornography) industry to ensure that adult content providers understand the new law and comply with the age verification requirements. We also engaged with age verification providers, ISPs, Mobile Network Operators, Payment Service Providers and Ancillary Service Providers to make them aware of the implications of the new regulatory regime. A BBFC Age-verification Charities Working Group held its inaugural meeting in 2017. This group meets regularly and will help the BBFC follow an evidence-based approach to regulation. It will also assist with monitoring the impact of the legislation on child behaviour and protection.

6. Potential new models for online regulation

6.1 The BBFC will continue to look at how we can ensure more consistent use of our age ratings and advice online. We believe that the BBFC system of classification meets the key criteria for child safety online. Namely, having:

- child protection at the core;
- effective labelling of content so that the standards are trusted and understood because they reflect national sensitivities and the symbols used are recognisable;
- broad coverage so that the system creates a known standard;
- low cost; efficient, flexible and innovative service so that it can keep pace with technological change and not be burdensome on industry.

User Generated Content

6.2 The BBFC supports the principle of working with industry to achieve voluntary self-regulation to make the internet safer where possible, in line with the self-regulatory initiatives the BBFC has already instituted.

6.3 In recognition of the fact that user generated content (UGC) is an increasingly significant source of content online, the BBFC and the Dutch regulator, NICAM, have developed You Rate It (YouRI), originally at the request of the EU Commission's CEO Coalition to make the Internet a better place for kids. YouRI is a tool that provides age ratings for UGC available via online video-sharing platform services. The tool is a simple questionnaire, designed to be completed by those uploading videos onto a platform, or by the crowd, or both. Those who use it are asked six questions about the content to be rated. Algorithms then automatically and immediately generate nationally sensitive age ratings and content advice. The tool, and the methodology behind it, is scalable to a global basis. The questionnaire itself would be the same in each country or territory but it produces bespoke, national ratings and content advice that take into account cultural and societal differences. It is a low cost means of capturing the enormous, and rapidly expanding, amount of UGC content that is not currently being rated, and is not susceptible to being rated under other models operated by ratings bodies around the world. The tool can also be linked to parental controls. Further information can be found at: http://www.yourateit.eu.

6.4 The BBFC and NICAM have completed a successful pilot project with the Italian media company Mediaset, and now need new industry partners to develop and test the questionnaire more extensively. EU Kids Online research shows that children are concerned about accessing unsuitable content on UGC video hosting services. The BBFC believes YouRI is a template which could be tested further in the UK/Europe through a pilot programme if industry partners are willing to participate in a trial project.

6.5 In relation to the Government's proposals on transparency in the Internet Safety Strategy Green Paper, the BBFC would also urge that there is reporting on the labelling of content using trusted national standards which can be linked to parental filters. Trusted labelling of content would enable action taken by video sharing platforms, including social media companies, to have a direct and very practical benefit enabling parents to protect their children from potential harmful content through parental controls.

Music Videos

6.6 In response to public concern, in 2014 the Government strongly encouraged the voluntary classification of music videos that were unsuitable for younger children. The BBFC, Vevo, YouTube and the three major UK record labels therefore launched a pilot scheme. Since then the BBFC has also been working with the major UK record labels to offer 24 hour turnaround and reduced cost classifications for music videos to ensure online music video platforms can display trusted and understood age ratings. The UK's independent labels joined this process in 2016, though the participation by the independent labels is less consistent. The number of music videos submitted was 100 in 2015 but declined to 51 in 2017.

6.7 The concept of age rating online music videos is accepted by all three UK major record labels. However, this initiative would be more effective if US and other international repertoire were brought into the scope of the process because currently some of the most prominent and controversial music videos are not receiving classification. In addition, there could be more prominent age ratings on platforms tied to parental controls.

7. Education and online safety

7.1 The BBFC believes education in schools is vital in contributing to building children's resilience in dealing with online risks, including age inappropriate content. The BBFC Education Team seeks to promote resilience in schools through its education outreach programme. The BBFC has spoken face to face to over 50,000 people in the past five years, more than 75% of whom are under 18. The BBFC also provides curriculum-based resources for schools and offers a dedicated children's website, www.cbbfc.co.uk. Through these various platforms, the BBFC explains to children, parents and teachers how to find out about age ratings and make safe viewing choices online. The BBFC works in partnership with organisations such as Childnet to provide parents and children with guidance, including through Safer Internet Day. The BBFC is also developing with the PSHE Association an accredited PSHE resource designed to promote resilience and making good choices. It will include lesson plans and a teacher pack.

8. Conclusion

8.1 The BBFC supports regulatory initiatives to make the internet at safer place and particularly the focus on the need to protect children from potentially harmful material online. The BBFC's experience is that consumers expect and prefer protections offline to be replicated online. The BBFC would urge the Lords Communications Committee to consider further the value of trusted systems for labeling of content, which reflect national sensitivities and can be linked to filters and parental controls. The BBFC believes the YouRI tool could be an ideal pilot under the internet safety strategy and would welcome a partnership with industry. The new regime of age-verification for commercial pornographic services under the DEA directly addresses core concerns about children accessing pornography and will substantially reduce the risk of them doing so. In relation to this new age-verification regime, the UK is leading the way and will set an international precedent in child protection.

11 May 2018

BCS, The Chartered Institute for IT – written evidence (IRN0092)

BCS is here to Make IT Good for Society. We promote wider social and economic progress through the advancement of information technology science and practice. We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

The following evidence to the Committee has been written after consultation with our 70,000-strong professional membership; including experts within our Legal, Internet and ICT Ethics specialist member groups.

Q1: Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

1. With regard as to whether internet regulation is desirable; it is important to differentiate between regulating the internet as a whole and regulating content that is hosted on the internet. While the former is very difficult and of questionable desirability, the latter still presents difficulties, but has near unanimous agreement.

2. Ensuring that extreme content, such as that with incites violence or child pornography, is removed from platforms as quickly as possible is obviously necessary. However, many issues of online content are already subject to existing legislation and enforcing these rules and bolstering their effectiveness may lead to faster results than creating brand new online specific regulations. For example, a post that is transgressing libel laws will do so whether or not it is hosted on the internet.

3. The global nature of the internet will always make effective regulation difficult and any question of its efficacy must consider the scope for international collaboration on whatever regulation is being proposed. Producing legislation unilaterally, however well-conceived, will not solve many issues of note. An example of this is intellectual property; often, those who are in breach of the law in one country are able to locate themselves in another where intellectual property laws are less stringent[384].

4. Additionally, even when there is harmony in regulatory frameworks between countries, it is still not always clear where jurisdiction lies in enforcing rules, such as in pirated content. Respondents to our consultation felt that for major regulation to have a chance of success, there would need to be a critical mass of countries willing to implement it. This would mean a grouping of the size and influence of the G7, European Union or an equivalent international organisation.

5. There are also significant technological issues around potential internet regulation, both in terms of enforcement and the number of people who successfully circumvent laws; a case in point are peer-to-peer (P2P) sites such as 'ThePirateBay', that are largely used to disseminate content illegally. The

[384] http://openaccess.city.ac.uk/17914/1/Hitsevich%2C%20Nataliya.pdf

Intellectual Property Office estimates that 15% of UK internet users over the age of 12 (equating to around 6.5 million people) have consumed illegal content within the past three months[385]. This is despite a concerted effort by both the UK government, the European Union and Internet Service Providers (ISPs) to block P2P websites over several years[386].

6. This is partly because evading such blocks is a trivial process for people with a rudimentary knowledge of the internet and a small amount of time. Even if efforts are redoubled to prevent these sort of websites, it is hard to envision a situation where they will successfully be snubbed out; both because the infrastructure of the internet will not fully allow it and because there will be people developing how to evade blocks. It is difficult to envision regulation of the internet ever being watertight because of these factors.

Q2: What should the legal liability of online platforms be for the content that they host?

7. There is a growing consensus that online platforms have a responsibility to their users and the wider world. Considering the massive role these platforms (and the companies that run them) have in everyday life, the fact that they are online should not preclude these responsibilities, including legal liability for content on their platform.

8. There is already legal liability for certain content like libellous posts for platforms if they have been notified of such content and have not acted upon this information, as outlined in the 2001 Godfrey v. Demon Internet Limited case[387]. Where there is a greater lack of clarity is in terms of abusive and extreme content, particularly when posted on social media and the respective responsibilities between the platform and the person who posted the offending work.

9. For wider legal liability of content online to be fair, it would need to follow a route of being contingent on the platform being aware of an issue and not acting upon this information in an agreed upon timeframe. For example, if someone posted an overtly racist picture on a social media website and this was then reported by another user, the platform in question should be at least partially liable for the ongoing impact of that post and must take appropriate action to mitigate that impact.

10. Dictating the appropriate amount of time between something being reported and dealt with prior to the platform being in contravention of the law is not simple and would require consultation between relevant stakeholders first. The example of Germany's NetzDG law that enabled fines of up to £44 million for platforms that failed to remove hate speech within 24 hours illustrates what can happen when this sort of law is enacted without enough consultation[388]. Due to

[385] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/628704/OCI_-tracker-7th-wave.pdf

[386] http://www.wired.co.uk/article/pirate-bay-court-block-europe

[387] https://globalfreedomofexpression.columbia.edu/cases/godfrey-v-demon-internet-limited/

[388] https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in-spotlight

the scale of the potential fines, companies have blocked more content than is necessary, creating issues around freedom of speech and causing the law to be revised[389].

11. Consequently, any attempt to produce similar legislation on platforms in the UK ought to take special care to produce the right balance between security and freedom. A model for progress in this area could be similar to the proposals in the recent Internet Safety Strategy Green Paper; whereby a code of conduct between online platforms and government is agreed upon and failure to adhere to these standards would result in penalties being put into law through primary legislation.

Q3: How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

12. The variation in size between online platforms makes a definitive answer to the question difficult. Larger platforms have the resources to employ extensive teams of people to check content, with Facebook for example having around 7,000 people working within their moderating team[390]. It would not always be right to expect the same standards of punctuality from smaller platforms, although there must be a minimum level of service. One consistent theme from respondents was that moderating has a tendency to lack transparency and clarity across many platforms.

13. At this point in time, automated processing is not generally advanced enough to make a decision on whether a piece of content is worthy of deletion or not. As a result, there should still be an expectation that the act of moderating something should be performed by a human, even if technology flags up what a person then decides upon. Automated processing can also be utilised effectively to weight the likelihood of certain users producing inappropriate content and this can help to prioritise the sort of posts moderators will need to look at. Ultimately, larger platforms should be utilising all of the tools in their arsenal, both human and technological, to create fair and balanced moderating systems that inspire confidence.

14. Respondents felt that there were often inconsistencies in the approach of platforms to moderating inappropriate content, with certain things such as nudity seeming to be resolved faster than posts that target people based on religion or ethnicity. Part of this can be attributed to the relative ease of identifying whether certain forms of content are against the rules as compared to others, but greater consistency in all types of cases being addressed would be welcomed.

15. Having procedures in place so that people whose content has been removed have the right to appeal is essential to a good moderating structure. As in the

[389] https://www.reuters.com/article/us-germany-hatespeech/germany-looks-to-revise-social-media-law-as-europe-watches-idUSKCN1GK1BN

[390] https://www.ft.com/content/400414f8-300e-11e7-9555-23ef563ecf9a

case of people who have reported something, those who have had content removed should also see their appeal resolved within a reasonable timeframe.

16. A number of respondents mentioned the need for an institution that could act as a neutral arbiter if a case reaches the end of an escalation process without resolution. Recent experience has shown that leaving platforms to moderate themselves does not always create results that meet public expectation and a neutral institution would give users an independent avenue to appeal. One solution would be to create an ombudsman service, possibly as part of OfCom, that would decide on these sorts of cases.

Q4: What role should users play in establishing and maintaining online community standards for content and behaviour?

17. There is a lack of awareness and understanding for many people in relation to their rights and responsibilities online and this will limit attempts to develop and impose online community standards that are effective from the grassroots up. For example, around half of internet users are unaware of what does and doesn’t constitute an illegal download[391]. This is not to blame users, but an honest appraisal of the current situation is necessary if appropriate measures are to be put in place that will catalyse an online community where users can be increasingly involved and invested.

18. Improving standards and behaviours is predominantly dependent on increasing public awareness of online rights and responsibilities and this could be partly achieved through awareness campaigns. The government has already invested in major campaigns relating to online safety, such as Cyber Aware, so the infrastructure is available[392]. A similar campaign for online behaviour would help raise awareness and the likelihood of people being able to identify what is in contravention of online rules.

19. Respondents felt that with these sorts of awareness measures in tandem with a growing cohort of the population being frequent internet users, we will move towards a situation where users are empowered to take more of a role in defining standards in content and behaviour.

Q5: What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

20. With respect to safety; online platforms being proactive and appropriating adequate resources to those reviewing flagged content would be a good starting point. Too often efforts to improve moderating and safety have come following negative press coverage, rather than because platforms believe it is part of their corporate responsibility.

[391] http://www.comresglobal.com/wp-content/themes/comres/poll/Wiggin_DES_Data_28_March_2013.pdf

[392] https://www.cyberaware.gov.uk/

21. The importance of awareness and education in empowering people to know about their rights and responsibilities online is also highly relevant for online safety. Platforms should play a greater role in providing information about how users can stay safe while using them and do so in a manner that is clear to the average user; both in terms of the language in which the information is written and through it being placed somewhere easily accessible.

22. Freedom of expression and freedom of information are the bedrocks upon which the internet was built. Attempting to curtail these excessively is not only in contravention of its design, but also liable to fail due to the ingenuity of internet users and the very infrastructure of the internet not allowing it. Resultingly, finding the correct balance between protecting individual liberties and ensuring safety is of vital importance, both for online platforms and in any attempt at designing internet regulations.

23.Consequently, platforms need to put in place structures that instil confidence to users that they both won’t be subject to arbitrary censorship, while also providing a better standard of safety than often exists currently. While this is not an easy task, it is far from an impossibility through increased effort and investment, in particular for the largest online platforms.

24. Respondents overwhelmingly believed that the maintenance of free speech was paramount to the ongoing creation and flourishing of online platforms. While being in agreement that certain content, such as that which incites violence, must be removed; legitimate criticism and platforms not allowing heterogeneous views would be hugely detrimental. Online platforms should be responsible for policing illegal material and not what is merely controversial for the most part.

25. Although the appetite for new internet regulation was varied among respondents, it was felt that codifying the rights that individuals should expect on the internet would be a welcome step. While legislation focusing on the internet frequently means limiting what platforms can do, it can take this more positive form. This is not without precedence, with the United Nations having declared that disconnecting people from the internet is a violation of human rights, affirming as a result that access is in of itself a right[393].

Q6: What information should online platforms provide to users about the use of their personal data?

26. As a bare minimum all provisions from GDPR must be delivered. There was unanimity from respondents in believing that GDPR would improve the relationship between user and platform with regard to data, but many felt that more was necessary.

27. Raising confidence and understanding for people about what their personal data is, which organisations hold it and who they are sharing it with is important; both in allowing people to take control of what they want to share and restoring trust in online platforms. With public trust and confidence about

[393] http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

companies holding their personal data being a miserly 20%, there needs to be an alteration in the relationship between data subjects and data controllers[394].

28. Users should have access to all data being held about them and be able to opt out of it being used or shared, unless that data is critical to the functioning of the relevant online platform. In particular, making it easier to see whether your personal information has been included in datasets shared with third parties, irrespective of informed consent, would be a step forward.

29. Having information available without people being aware of its availability, or able to easily access it, defeats the object of giving people control over their data. Online platforms should be encouraged to make it clear to users about what they are doing with personal data and do so in a form that can be easily interpreted; having one without the other is not sufficient.

Q7: In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

30. There is a need for more transparency around business practices than is currently the case; in addition to a sustained attempt to improve awareness for people about how business practices will affect them. This will not be easy, as evidence shows that people are overwhelmingly unaware of what their data is used for and why data is as valuable a commodity as it is to many online platforms[395]. For example, academic studies show that up to 98% of people don't read terms and conditions on websites before submitting their details to a platform[396].

31. This is a huge gap to bridge that no one piece of regulation could achieve. However, as with personal data, GDPR will play a positive role due to its provisions around consent, although it should not be seen as the solution to everything. Additionally, the proposed internet safety transparency record will help, although its provisions need to be expanded to cover more than social media[397]. Across the board, platforms need to be explicit in what they are doing with data, especially when it is being used significant profit.

32. Regarding the role of algorithms specifically; there is a danger of companies technically being more transparent through releasing details, while not necessarily providing clarity to the public. It is not enough to release lengthy and complex technical detail to people, the majority of whom are not technical experts, without some attempt to explain how the algorithms pertain to their experience of the platform in question. Consequently, a more fruitful approach would be to ensure that platforms are open to users about how their algorithms are used and why. For example, if a social media platform is collecting some profile data in order to target adverts, this needs to be understood by users. Companies should also be able to both identify and explain why an algorithm has

[394] http://www.comresglobal.com/polls/information-commissioners-office-trust-and-confidence-in-data/

[395] https://www.citizensadvice.org.uk/Global/CitizensAdvice/Consumer%20publications/Personal%20data%20consumer%20expectations%20research.docx.pdf

[396] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465

[397] https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2017-10-11/HCWS156/

produced any individual result, something increasingly difficult with the rise of more complex algorithms being used in AI and machine learning.

Q8: What is the impact of the dominance of a small number of online platforms in certain online markets?

33. The internet tends towards monopoly in numerous areas. It is not realistic, especially at this juncture in the internet's existence, to expect this to change as most monopolistic platforms have a global reach outside of the control of one country. In many respects, this is not that different from other corporations in a globalised world and the approach to take with entities that have this level of market dominance is much the same; ensuring that these platforms have responsibilities to their users and the world as well as their shareholders.

34. There are undoubtedly some negative results from this level of dominance, such a lack of consumer choice and motivation for improvement. There have never previously been so few companies with such overarching control of global communication and data. The main concern is that some platforms now control such an amount of critical infrastructure and communication systems that it stops alternatives from ever being able to succeed.

35. One example of the issues around platform dominance is Amazon Web Services, that utilises Platform as a Service (PaaS)[398]. This involves software teams writing code to directly interface with the Amazon Service. To move that away from Amazon, would likely turn into a multi-year project of re-writing a significant amount of an application or service, while being at the mercy of Amazon changing things in the interim. Ultimately, there is a danger of companies being beholden to one supplier, as there is not at alternative platform that people could use.

Q9: What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

36. Generally, respondents believed that the UK leaving the EU will likely have a negligible to mildly negative influence on internet regulation in the UK in the short term, but that there is the potential for this to arrested through a proactive approach. The point was made that even if we do stop being party to certain regulations after Brexit, it would be easy enough to transplant these into UK law if there is the will to do so.

37. Maintaining EU regulations with regard to data and the internet are important to ensure a frictionless relationship, especially in trade, between the UK and the EU following Brexit[399]. However, merely following existing standards should be a bare minimum and the UK should take the chance to be an exemplar and innovator in terms of our internet regulatory environment. The commitment of the Department for Digital, Culture, Media and Sport (DCMS) to look at

[398] https://aws.amazon.com/types-of-cloud-computing/

[399] http://policy.bcs.org/sites/policy.bcs.org/files/Digital%20Brexit%20Text_WEB_1.pdf

improving the regulation of major internet platforms following Brexit suggests this may well happen[400].

38. This positive attitude towards moving away from EU regulation is contingent on the UK using Brexit as an opportunity to enhance the individual's online experience. There were concerns that it might be alternatively seen as a chance to strengthen the ability of platforms to profit from the internet instead. One example given of a negative change that could be enabled by Brexit was the watering down of existing EU net neutrality rules in favour of a model that would benefit ISPs by further monetising internet access[401].

May 2018

[400] https://www.theguardian.com/media/2018/mar/14/uk-could-rethink-social-media-laws-after-brexit-says-minister

[401] https://berec.europa.eu/eng/netneutrality/

Dr Paul Bernal, University of East Anglia Law School – written evidence (IRN0019)

I am making this submission in my capacity as Senior Lecturer in Information Technology, Intellectual Property and Media Law at the UEA Law School. I research in internet law and specialise in internet regulation from both a theoretical and a practical perspective. My first book, *Internet Privacy Rights – Rights to Protect Autonomy*, was published by Cambridge University Press in 2014. My second book, *The Internet, Warts and All: Free Speech, Privacy and Truth*, which will be published by Cambridge University Press this summer, has the question of regulation of the Internet as one of its central themes. The subject of internet regulation therefore lies precisely within my academic field.

Brief summary of this submission

This submission notes that to a significant extent the internet is already regulated, and we need to be clear about that so as not to let people think that it is some kind of 'Wild West' overrun by rogues. It also suggests that though in some ways further internet regulation is necessary, those regulating need to be very wary of doing so. There are a number of significant risks attached, including:

(1) Of overregulation, stultifying areas of expansion and benefit to the community and to business;
(2) Of regulation missing its targets and having significant and damaging consequences in other areas;
(3) Of creating misleading and unhelpful expectations in the eyes of the public, potentially reducing their ability to navigate the complex environment;
(4) Of creating opportunities for regulatory arbitrage;
(5) Of the regulators being subjected to significant lobbying; and
(6) Of incurring significant and unnecessary expense.

This does not mean that regulation should not be considered – particularly, for example, on algorithmic accountability - but it needs to be taken very seriously and monitored very closely if a decision is made to regulate. Where regulation is not working or being counterproductive, it needs to be reversed. The possibility of that kind of reversal needs to be built into the regulatory system from the offset.

There has been more focus upon the role of online platforms and intermediaries in relation to their content (including hate speech, copyright infractions, obscenity and pornography, extremism etc) than on the delivery methods and the way that they often rely upon access to and use of personal information. That betrays a limited and somewhat old-fashioned understanding of the internet, considering it in terms of 'publishers' or 'platforms' – the question seemingly often asked being 'should we consider them as publishers, with all the responsibilities in law that this implies'. That, this submission will suggest, misses the key point. That systems like Facebook host material is less important than the way that the material reaches its intended audience – through targeting based on profiles from personal information, either directly or automatically through Facebook's tailored news feeds and so forth. The use of personal information is the key that unlocks the audiences, enables political manipulation by things like fake news and so forth. It is the underlying systems that underpin the problem: regulating the content without looking at this is to a great extent like rearranging the deck chairs on the Titanic.

1 The Internet is already regulated

1.1 It is important not just to understand but to make clear to others that the internet is already regulated by a wide range of laws, from those governing speech (such as S127 of the Communications Act 2003, the Malicious Communication Act 1988) and public order law to data protection, copyright and fraud, as well as civil law such as defamation law, misuse of private information and much more. It is a commonly held and unfortunate belief amongst some that the internet is a lawless 'wild west' where the law does not apply. It does, and some of that law works very well. Regulatory bodies such as the ICO and Ofcom have powers that function on the internet, there are quasi-regulators such as the Internet Watch Foundation and more.

1.2 What this means is that parliament should first be considering how well the existing regulation works before considering further regulation. Rationalising law where there are overlaps and confusion (for example over speech), strengthening laws and putting more resources into enforcement and so forth where it is needed – the ICO in particular is distinctly under-resourced for the critical tasks that it has to perform in the internet era.

1.3 It also means that emphasis should be placed in making sure that all of those involved in the process – and this starts with MPs, for example – have a better knowledge and understanding of the technology, of the environment, of the regulation and law that exists, and of the problems surrounding that regulation and law. The record in the recent past on this is not very good, from inappropriate prosecutions (such as the so-called 'Twitter Joke Trial', R. v Chambers) to laws that essentially fail (such as many parts of the Digital Economy Act 2010). Getting this right is critical before considering further regulation or legislation.

2 The risks of regulation

2.1 When considering regulation, the risks of that regulation have to be considered as well as the potential benefits. In relation to the internet, this is particularly pertinent, as the risks are multifaceted and often hard to quantify. Regulating intermediaries (including 'platforms' – though the term 'platform' is itself a loaded one, implying a lack of responsibility for the content) has many such risks, most directly that any restrictions on their actions could end up being restrictions on all their users – and to most intents and purposes that means all of us. We have grown to rely on these intermediaries for many aspects of our lives – if their actions and activities are restricted then so are ours.

2.2 Further to this, one of the biggest risks is that regulatory action will fail to find its targets but instead hit 'innocents'. A highly skilled malicious actor will be able to avoid or sidestep regulatory action, but the regulation might catch innocent and positive people instead. Sex education websites can be blocked by porn-blocking systems whilst those distributing child-abuse images bypass the systems by using the dark web, for example.

2.3 Regulation can also create false and damaging expectations. If a parent is told that the new law will make sure there is no damaging material on the internet they may be less likely to pay proper attention to what their child is doing on the internet, for example. As I discuss in depth in my new book, *The Internet, Warts and All*, the internet is a messy and sometimes confusing place, and will always be so, which makes it vitally important that the emphasis is placed first and foremost on education and understanding. Our children need to become 'savvy' and encouraged to be sensible, rather than our suggesting that we can make the environment fundamentally safe. Similarly, consumers of news on the internet need to become savvy at understanding what they are seeing, if we are to address the issues surrounding 'fake news' (see section 4 below).

2.4 Regulation can also create opportunities for 'arbitrage' – playing one regulator against another, choosing which jurisdiction to base an operation in based on the local regulations. This can result in a kind of 'race to the bottom' – one of the risks associated with Brexit (see section 8 below). It can also mean a loss of business opportunities where regulation is excessive or inappropriate.

2.5 Regulators and lawmakers can also be pressurised, whether directly or indirectly, by powerful lobbies. As the committee is aware, the dominance of a small number of online platforms is one of the characteristics of the internet in its current form: this also means that the small number of very powerful companies that own these platforms have a very significant lobbying power, one that they often wield with great expertise and effect. That can mean that regulations fail to achieve what they need to achieve because the lobbyists manage to persuade those drafting the regulation into shaping it into a form that suits those companies. The massive lobbying budgets of Facebook, Google and others exist for a reason: part of that reason is to try to shape any regulations that are put into place.

3 Online 'platforms' and their responsibilities

3.1 Online platforms are already to an extent responsible for the material they host. Many kinds of material have to be removed under a range of laws. Google's transparency report includes take-downs on the basis of copyright, on the basis of government requests, and on the basis of 'right to be forgotten' claims under data protection law following the 'Google Spain' case. ISPs use the Internet Watch Foundation to block access to child abuse imagery. The idea, therefore, that intermediaries (including 'platforms') can be held responsible for content has been established and accepted, albeit in relatively limited circumstances.

3.2 How this might be taken further is another matter. It is important to understand that it is a very slippery slope, and that there could easily be a chilling effect on freedom of speech if it is taken too far. A platform may be cautious about hosting, reducing the opportunities for people to find places to host their material if it is in any way controversial. Again, issues like sex education, minority rights, politically contentious material such as that relating to dissidents or people who do not fit with a particular orthodoxy should come into play here. The result is therefore that power balances are exacerbated – the already powerful and orthodox find their platforms easily, those without power find it very hard. As one of the primary functions of freedom of speech is to allow the relatively weak to face up to the powerful, this is of great significance. It means that extending responsibility to the platforms into more areas should be done with great caution.

4 Fake News and other misinformation

4.1 A particular area of importance in relation to the online platforms is their role in relation to fake news. It is important at the outset to understand that there has always been fake news – and there always will be. Examples can be found from almost every period of history, from the false stories spread about Oliver Cromwell by his Royalist adversaries and the subversive rumours spread about Cardinal Mazarin in 17th century France to the broadcasts of Lord Haw-Haw and the press conferences of Iraqi Information Minister Muhammad Saeed al-Sahhaf, known as ‘Comical Ali’. It is not possible to stop people from creating stories about their political enemies – and these days it is particularly easy to do so. Websites, and Facebook pages in particular, can be created in minutes.

4.2 The existing mass of media, and the narratives created by it, provides a fertile ground and much ammunition with which to craft the false but convincing stories that constitute much fake news. It is important to understand that the ‘new’ form of fake news works with rather than against the traditional media. A headline story in the Daily Mail, whether true or not, might be used as the basis of another, wholly false story. It is important also to understand that the ‘news’ presented by the traditional media can easily be as ‘fake’ as that found on the internet – or it may be used to create a narrative that is essentially fake, even if the particular facts used are actually true, though taken out of context or misinterpreted.

4.3 This means that taking measures against ‘fake news’ whilst not addressing the fake narratives that are already in circulation is doomed to failure. More fake news can be created very fast, and posted up as soon as it is created, ready to be spread around the internet in a matter of moments. Dealing with just the content is little more than a doomed game of ‘whack-a-mole’.

4.4 Fact checking and labelling fake news does not help. The empirical evidence shows labelling something as fake can actually make it more likely to be read and more likely to be believed. This may be to do with just the highlighting, or to do with a label being seen as a ‘badge of honour’ that the piece is not trusted by the ‘mainstream’ or the ‘elite’. This means that any measures to require platforms to fact-check and label fake news are likely to be not just ineffective but actively counterproductive.

4.5 The underlying problems with fake news are not the content but the mechanisms of distribution. The way that Facebook 'tailors' its news feed to your 'interests' means that fake news in your interest area will be actively pushed to you. If you have shown, for example, a particular interest in what you see as problems with immigration, stories about immigrants committing crimes or being given massive amounts of benefits will be algorithmically selected to be suitable for you – whether they are true or not. Fake news creators know this and can craft their stories to work in this way.

4.6 This in turn relies on the profiles built up on users based on their personal data: if they cannot profile people as precisely, the fake news cannot be targeted as accurately. This has big implications in relation to political manipulation to: the Cambridge Analytica saga, so far as we can determine started with big data analysis of people's personal data to derive political opinions and finished by using that data to target individuals with both fake news and other content.

5 Online behaviour and safety – dealing with trolls

5.1 There is a qualitative difference between dealing with content and dealing with behaviour: targeted aggression, bullying and so forth are not so much about the specific content as they are with how that content is used, how people interact with each other and so forth. That means that regulation of it is also qualitatively different. As noted above, there is already a considerable body of law (both statute and case law) governing this kind of behaviour: what is needed most is an improvement in understanding and implementation of that law.

5.2 The social media companies are also already putting a considerable effort into dealing with these kinds of problems on their platforms. It is neither fair nor true to suggest, as is often done in the media, that they are not really trying. They are, and it should not be surprising that they are, as the success of their platforms relies on their not being hostile environments for their users. That they do not always succeed is mostly a reflection on how difficult a task it is, not on their failure to try. Part of the problem is that it is easy for arguments to become heated, and also easy for people not to understand how their actions appear to others: many 'trolls' have no idea that they are 'trolling'.

5.3 There are two particular findings from research that should be noted in this area. The first is that the superficially attractive idea of enforcing 'real names' on the internet (and on social media in particular) is not just unlikely to succeed but could even be counterproductive, as well as having devastating effects on certain vulnerable people. A key empirical study showed that when forced to use real names, trolls can become even more likely to be aggressive in their language and actions – whether from bravado or to make a point, or some other reason. In addition, forcing real names puts many people at risk, from those with abusive spouses to whistle-blowers, from those with names that indicate their ethnic, religious or other background – or simply to women and girls operating in oppressively male environments, of which there are many on the internet. It is no coincidence that one of the methods of the most aggressive trolls is 'doxxing' – finding and releasing personal information about their victims to scare them or even cause them harm. 'Real names' policies help doxxing.

5.4 The second, which fits with this latter point is that tools created to 'deal with' trolls – whether they be software tools such as 'report abuse' buttons or legal tools as mentioned above – can end up being used *by* trolls against their victims. A troll will report their victim as a troll, in the hope of getting them banned from a platform or worse. This means that providing more such tools needs to be done with a great deal of care, or it may simply make the trolling situation worse.

6 Personal data, privacy, and its critical role

6.1 As noted above, the gathering and use of personal information underpins many of the worst problems on the internet at present. Privacy invasion and profiling lies behind the fake news phenomenon and the broader issue of political manipulation (as graphically illustrated by the Cambridge Analytica saga), as well as providing tools for scammers and other criminals, creating vulnerabilities that can be exploited and much more. It is critical that privacy is not downplayed or seen as playing second fiddle to issues such as security and freedom of speech. It matters as much in its own right and also supports those rights and issues. Without privacy it is very hard to have security, and without privacy it is hard to have real freedom of speech. A lack of privacy causes a chill in free speech – not just theoretically but in practice, as has been demonstrated through a series of empirical studies.

6.2 Privacy and personal data is also an area where extensive law already exists. Data protection law, and in particular the new General Data Protection Regulation, has the potential to provide a good deal of support for individual privacy – but only if it is enforced with sufficient rigour and support. The Information Commissioner's Office ('ICO') needs to be given more resources both in terms of finance and expertise, and perhaps more responsibilities. If the ideas of algorithmic accountability and algorithmic audit (see section 8 below) are to be both useful and appropriately independent, the ICO is likely to be the best body to oversee them. This, together with the growing responsibilities in relation to data protection, means that they will need much more support.

6.3 Asking what information online platforms should provide to users about the use of their personal data is only part of the question that should be asked. What is more important is what they actually do with that data: people will generally simply scroll through whatever information is provided and click 'OK' at the end. Regulation of the use of personal data based on information and 'consent' is not sufficient: it is more important to set clear and strong rules about what is and is not allowed. It is also important to understand that it is not just how the information is used directly, but what can be derived from it, and the profiling and targeting practices of the platforms that need to be addressed.

7 The dominance of a small number of platforms.

7.1 The domination of the online world by a few platforms owned by even fewer corporations (Instagram and WhatsApp owned by Facebook, YouTube owned by Google, for example) has many implications. It means that their methods have a massive impact on the online world – and that they have immense power, some of it wielded through their market domination, crowding others out, some wielded algorithmically as they control what we see, read and hear. What appears on your Facebook news feed, or at the top of your Google search results or in predictive text as you search, has a massive influence over the information that you see and consume. It is critical to understand that the algorithms that determine these are not in any real sense neutral, objective or 'organic', and neither are they purely 'crowdsourced'. They are the result of design and decisions by people employed by the companies.

7.2 Part of the reason for this dominance is the effectiveness of the services – but part of the effectiveness is caused by the dominance. The number of users and the amount of data gathered by and through those users makes the profiling and other big data analyses more effective. It makes the search results better and so forth. The more data the companies have, the more they can derive – and the more effectively they can use it. Sometimes this is very positive – but it also opens dangerous possibilities. The more 'base' data on a population that is available, the less specific data on a particular individual is needed to profile them. This, again, is fundamental to understanding how the kind of targeting used by the likes of Cambridge Analytica works. It is also important to understand that this also means that deeply sensitive data – from data about health to sexuality and political views – can now be derived from the most mundane information about shopping habits, tastes in music and so forth. That in turn means that providing protection only for the directly sensitive data will not protect individuals in practice.

7.3 The size and strength of the companies behind the platforms, as noted in 2.5 above, gives them massive lobbying power. Lawmakers and regulators need to be able to resist this power – and in particular resist the temptation to give these companies special access, private hearings and so forth.

8 Algorithmic transparency, accountability and audit

8.1 Perhaps the most important area where further regulation needs to be considered concerns algorithms. The power of the algorithms of the internet giants – search engines like Google and social networks like Facebook in particular – has already been noted above. That these algorithms are treated effectively as trade secrets, 'black boxes' that we cannot see into, should be seen as increasingly untenable. If they have so much influence on our lives means that the companies that control them should be accountable for them – much more so than they should be held accountable for the content hosted on them. It is the algorithms that lie behind the effectiveness of the products and underpin the business models of the companies.

8.2 Being accountable for the algorithms includes more transparency as to how the algorithms are used – not the technical details, but the things that they are used for. People need to be made properly aware, for example, that algorithms curate their news, and the overall aims of that curation – and not in terms like 'we tailor news to better match your expectations' but more realistic assessments acknowledging how profiling is done and so forth. Transparency, however, is not enough. It will very easily become little more than the 'scroll down, don't read, then click OK' procedure that is supposed to constitute consent. What needs to be considered is 'algorithmic audit', where algorithms are regularly tested by an independent auditor – not analysed for their technical content, which should rightly remain effectively a trade secret – but for the results that they produce.

8.3 How that independent audit would function would need a lot of thought and expertise. Which algorithmic systems need to be audited, and when. Who would be qualified to perform these audits, and how would the results be communicated. This in turn requires a regulator with the power and resources necessary to make it work. The ICO is the most obvious body to oversee such a function, but it would need considerably more resources than it currently has, reporting responsibilities to parliament on this, and power to enforce both the requirement to algorithmic audit and the results of the audit itself. The role of algorithms is only going to grow and become more complex – particularly with the growth of 'machine learning' and 'artificial intelligence' (and the grey areas between them). This makes addressing this issue of critical importance. As noted above, it has more impact on many of the areas for which regulation is being considered than regulating the hosted content itself. Moreover, there is no existing regulation in the area, unlike such things as extremism, hate speech, obscenity and copyright infringement.

9 Brexit and related problems

9.1 The primary impact of Brexit on internet regulation is negative – it creates gaps in regulation that could be exploited, could provide opportunities for regulatory arbitrage and could reduce the ability for regulators to take on the giants of the internet. The European Union has much more strength to resist the lobbying of the internet giants, and much more capacity to punish them through law. The new fining capabilities in the GDPR are the most recent example but there is an effective track record through competition law, including a €2.4 billion fine to Google in 2017 over the Google Shopping case. That sort of strength is unlikely to be possible for UK regulators outside the EU.

9.2 The best that can be done to limit this is to ensure that the UK aligns itself as closely as possible with the EU in regulatory terms. Lawmakers should resist the temptation to differentiate the UK from the EU, particularly in terms of data protection and electronic commerce, even if it perceives weaknesses in EU regulations – any marginal advantages are likely to be miniscule in comparison with the advantages of regulatory harmony and shared lobbying power, as well as potentially driving a 'race to the bottom' in terms of regulation of the big internet companies. This also means that the UK should be willing to adjust its surveillance practices and law to make GDPR adequacy more likely. Access to the digital single market is another aspect of this – again, if Brexit means that the UK loses these advantages it could have a seriously detrimental impact in both economic and regulatory terms.

10 Conclusions

The most important thing to understand is that bringing any further regulation into the internet should be considered very carefully. Regulation could very well be counterproductive, have serious side effects and have an impact on privacy, freedom of expression and a wide range of other human rights whilst failing to deal with the real problems. We use the internet for so many different parts of our life that anything done to regulate it – to restrict it in particular – can have an impact on all those things. For this reason, the default position, particularly insofar as regulation of content is concerned, should be *not* to regulate rather than to regulate. Freedom of speech should be the starting point. Moreover, the regulation of content on its own may be a fruitless task: in most cases similar content will reappear and be spread throughout the net. The negative side effects may well be the only real effects.

The two areas where this is not true, are the protection of privacy and the regulation of algorithms. Privacy underpins many of the issues that should be of concern – including fake news, trolling, the excesses of power of the internet giants, the potential for the undermining of democracy as demonstrated by Cambridge Analytica and more. There is already good law in this area – data protection law – which should be supported and more strongly enforced. More resources for the ICO, and encouragement to the ICO to use its enforcement powers, would be very much a positive. The regulation of algorithms is something that needs to be addressed and addressed soon. The power of algorithms and their influence in many different areas of our lives is growing all the time: the discussion about how to deal with them needs to begin now.

There has been a lot of academic research into a number of these areas, and the evidence from it may sometimes seem counterintuitive – the idea that 'real names' policies are likely to make trolling worse rather than better, for example. This make it important that lawmakers and regulators engage with the research community, including both academics and NGOs. Being willing to take in even the more counterintuitive research results will mean that regulation, should it be deemed necessary, should be more effective, with fewer bad side effects and less likelihood to need reassessing and reversing in the future.

I hope this submission is of use to the committee, and I would be happy to provide more detailed information, either written or oral, should the committee wish. This could include links to the relevant pieces of empirical and other academic work referred to, and subject to permission from my publisher to drafts of the relevant chapters of my forthcoming book that cover some of these areas – fake news and trolling in particular – in some detail.

10 May 2018

Big Brother Watch - written evidence (IRN0115)

About Big Brother Watch

Big Brother Watch is a cross–party, non-party, independent non-profit organisation leading the protection of privacy and civil liberties in the UK. We expose and challenge threats to people's privacy, freedoms and civil liberties at a time of enormous technological change in the UK.

Introduction

1. Internet and social media companies have become central platforms for discussion and debate, for information access, for commerce and increasingly even human development.[402] This has given internet and social media companies – primarily a small number of global, for-profit companies – a critical role mediating people's ability to freely express themselves and their opinions online. Existing regulatory frameworks applied to these global platforms range from diverging national laws to self-regulatory guidelines produced by internet companies themselves. Big Brother Watch believes it is entirely possible and desirable to construct a harmonious online environment where expression is free and people's privacy is protected, and where the rule of law is upheld.

Q1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

2. Firstly, it is important to acknowledge that the internet is a complex environment comprising communications networks, information storage and sharing, multiple forms of commerce, and many non-profit endeavours. The internet is an extension of society itself, and accordingly there is not simple or desirable way of 'regulating the internet' as a whole sphere. Indeed, many actions carried out on the internet are already subject to regulation in various forms. This is particularly the case with communications, which we wish to consider further in this submission.

3. Secondly, we believe that before deciding on a method by which to achieve change – regulation or otherwise - parliament, the public, and internet intermediaries still need to have a meaningful and engaging conversation about exactly what changes are needed to benefit society.

4. Big Brother Watch believes that the status quo needs to change. **We believe that internet intermediaries of a certain size, particularly social media platforms and search engines, should only restrict**

[402] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 6 April 2018 (https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf)

free expression to the extent that that right is limited in human rights law; and that any enforcement action should be safeguarded by transparent policies and clear and accessible appeals processes. Whether it is desirable or moreover possible to achieve that model via the provision of new regulation is an outstanding question. However, with or without regulation, there is much more Government and the intermediaries can do.

5. Social media companies have become the modern public square, whilst search engines are like supersized modern libraries. These internet intermediaries have enabled the open and democratised sharing of information, and provided platforms for people to speak truth to power. Social media platforms in particular have connected people to engage in politics, form communities, to share views and debate. With over two billion users actively using Google and Facebook respectively, these internet companies are operating at a magnitude whereby they function as part of our modern communications infrastructure – much like public utilities. Therefore, any regulation of these companies implicates people's rights to privacy, religious freedom and belief, opinion and expression, assembly and association, and public participation.[403] Accordingly, Government and the companies alike should ensure that people's rights and freedoms are protected, and that the same harms proscribed by law and dealt with in the physical world are dealt with on the internet.

6. Since internet intermediaries are our modern public squares and super-libraries, it is really important for the health of society and democracy that they are not regulated or interfered with beyond those basic human rights principles. 'Community values' are not appropriate for a platform hosting billions of users – the notion of one community in this context is a fiction. The fictional 'community' is a notion used to justify enforcement policies and actions that pertain to the legal protection or simply the brand identity of the platform. But in reality, there is not one online community, or one Facebook community, but many thousands of communities on these platforms each with different values, interests, and norms. To provide an inclusive platform where rights are respected, 'community values' should not be thrust upon such a large number of users - only the legal boundaries within which they live.

Regulation of expression must be based on international human rights law

7. As discussed, we believe that any regulation of online content on major internet platforms should be based on international and national human rights standards, with close regard due to the right to freedom of expression and the right to privacy which are particularly affected.[404] This is the most inclusive way to host diverse communities and

[403] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 6 April 2018 (https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf)

[404] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 6 April 2018 (https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf)

individuals, and to foster the open exchange of ideas, the development of views, and healthy debate.

8. The first step to adherence to human rights standards would be for the major internet intermediaries to pledge to follow such a model and open their processes and policies to independent inspection by expert bodies. The Government should actively support such a process.

9. We see no purpose in Government creating additional legislation to further restrict content, speech or other forms of expression online beyond the restrictions imposed by existing human rights law and the current roster of communications laws in the UK There are already a wide range of UK laws prohibiting violent and discriminatory forms of speech, including the Protection from Harassment Act 1997, Crime and Disorder Act 1998, Public Order Act 1986, Malicious Communications Act 1988, Communications Act 2003, and the Terrorism Act 2006.

10. It is already, for example, an offence to use "insulting words" whereby a person is "likely to believe that (…) it is likely that (*immediate unlawful*) violence will be provoked" - regardless of whether such violence is provoked (Public Order Act 1986, s.4). It is an offence to display "any writing, sign or other visible representation" that is "insulting" and causes a person "alarm or distress" (Public Order Act 1986, s.4A) or even "within the hearing or sight of a person likely to be caused harassment, alarm or distress" (Public Order Act 1986, s.5). Furthermore, it is an offence to send "a message that (*an individual*) knows to be false" for the purpose of causing "annoyance" or "inconvenience" (Communications Act 2003). Arguably, communications laws in the UK are already extensive and overly restrictive.

11. The vastly increased means by which to publicly exchange communications have given rise to unprecedented opportunities to monitor, regulate and restrict expression. As such, this is an important juncture for Government to consider reviewing existing laws that deal with the limitations on free expression to ensure that they are simple, accessible, compatible with Article 10 rights and conducive to a free and open society - rather than disproportionately censorious.

12. Government should apply UK laws dealing with the rights and limitations on free expression to the online sphere. The Director of Public Prosecutions' has already indicated that online hate crimes can be prosecuted to the same degree as offline hate crimes.[405]

13. It has been reported that Government is considering proposals to regulate 'non-illegal content'.[406] Any such proposals would clearly risk a disproportionate restriction on the right to freedom of expression. Big

[405] https://www.independent.co.uk/news/uk/politics/hate-crimes-social-media-crown-prosecution-service-home-office-prejudice-a7903166.html

[406] https://www.buzzfeed.com/alexwickham/uk-government-regulator-internet

Brother Watch will robustly oppose any regulation that would risk eroding or chilling that vital right.

14. We are also opposed to the fledgling proposals set out in two Bills set to have their second reading in Parliament on 26th October 2018: the Social Media Service Providers (Civil Liability and Oversight) Bill presented to Parliament by John Mann MP,[407] and the Online Forums Bill presented to Parliament by Lucy Powell MP.[408]

15. John Mann MP justified the necessity of his 'Social Media Service Providers (Civil Liability) Bill' with the argument that it's impossible for police to force Internet platforms to provide evidence in criminal prosecutions.[409] However this is incorrect, as UK police have the power to do so under the Regulation of Investigatory Powers Act 2000.

16. Lucy Powell MP's 'Online Forums Bill' is intended to combat private groups on social media that are considered breeding grounds for hate and proposes making group administrators and moderators legally liable for the content in those groups. Whilst there is certainly an issue with hateful content online, as there is offline, this fundamentally flawed proposal would undoubtedly result in a shrinking space for community groups to discuss and organise amongst themselves. The burden of legal liability would deter most communities from maintaining their online groups, worst affecting minorities such as LGBT groups; those who are vulnerable or already suffer discrimination, such as women's groups; and those who require on privacy and anonymity such as recovery or survivor groups, who rely on closed spaces for discussion and organisation. The problem of hate crime that Lucy Powell MP is understandably drawing attention to could, we believe, be dealt with under existing laws.

Regulation of targeted advertising

17. Big Brother Watch believes that parliament should consider passing an Act to prohibit micro-targeted advertising online. Targeted advertising is the practice of collecting data about internet users, including tracking users across websites and inferring their interests, in order to target tailored advertisements.[410] This practice is enabled by the vast monitoring and tracking capabilities in the online sphere.

[407] https://hansard.parliament.uk/commons/2018-02-28/debates/18022838000002/SocialMediaServiceProviders(CivilLiabilityAndOversight)#contribution-151690EC-1DCA-4C1F-BE73-4F28F260A08F

[408] https://hansard.parliament.uk/commons/2018-09-11/debates/BC2267F0-86BB-4746-B822-D6D8A55F31BF/OnlineForums

[409] "It is absurd that the police in this country cannot force Twitter, Facebook, Google or any of the others to provide evidence that is required for criminal prosecutions." 28 February 2018 (https://hansard.parliament.uk/commons/2018-02-28/debates/18022838000002/SocialMediaServiceProviders(CivilLiabilityAndOversight)#contribution-151690EC-1DCA-4C1F-BE73-4F28F260A08F)

[410] Toubiana, V, Narayanan, A, and Boneh, D, Nissenbaum, H and Barocas, S, 'Privacy Preserving Targeted Advertising' (2010). 'Proceedings Network and Distributed System Symposium', March 2010.

18. The very nature of targeting advertising, tracking and profiling users based on their browsing history; purchasing habits; sociodemographic traits such as age, gender, race, economic status; psychographic characteristics such as lifestyle, opinions and values; and geographic location is inherently privacy-invasive. To seek this level of detail about individuals' private lives for the purpose of commercial or political advertising is unethical and makes for an unhealthy online environment. In extremis, such targeted advertising could even jeopardise the integrity of our democratic processes – an issue raised by the Cambridge Analytica scandal this year**.**

19. For example, Facebook tracks users through 'Like' buttons across the internet, whether or not they are logged in, or even have a Facebook account;[411] it maintains shadow profiles on people who don't use Facebook;[412] and it tracks location and targets adverts based on where an individual is, where they live, and where they work.[413] Facebook allows advertisers to target people in several different ways: through their demographics, including "age, gender, relationship status, education, workplace, job titles and more"; their interests, including their "hobbies, favourite entertainment and more", whereby advertisers group users based on specific words shared on their timelines; through their behaviors, including "purchasing behavior, device usage and other activities", and their location.[414] For example, Facebook has allowed advertisers to run adverts that target only men or certain ethnic groups,[415] and has allowed predatory "conversion therapy" adverts to be aimed at vulnerable young gay men.[416]

20. Advertising provides a lucrative revenue stream for social media platforms, which is only growing as those platforms consume more and more human attention. However, advertising on specific platform webpages would also be lucrative, without needing to target adverts at the individual level. Big Brother Watch calls for a ban on micro-targeted advertising online.

Q2. What should the legal liability of online platforms be for the content that they host?

21. Internet platforms are not arbiters of the law – like other companies, they are subject to the law. In addition, social media networks and search engines are clearly not publishers, but intermediaries. Therefore,

[411] https://gizmodo.com/all-the-ways-facebook-tracks-you-that-you-might-not-kno-1795604150

[412] https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy

[413] https://www.eff.org/deeplinks/2018/04/facebook-doesnt-need-listen-through-your-microphone-serve-you-creepy-ads

[414] https://en-gb.facebook.com/business/products/ads/ad-targeting

[415] https://www.telegraph.co.uk/technology/2018/09/18/facebook-accused-discriminating-against-women-targeted-job-adverts/

[416] https://www.telegraph.co.uk/news/2018/08/25/facebook-accused-targeting-young-lgbt-users-gay-cure-adverts/

they should not be held liable for third party or user content on their platform that they were not involved in modifying, or for failing to identify illegal content. They should only be liable for failure to adhere to lawful orders, such as court orders to remove content.

22. Intermediaries' technical ability to perform a quasi-policing function does not equate to a legal or even moral responsibility to do so – nor would their fulfilling such a function necessarily benefit society. The line between free speech and censorship is delicately maintained and is an indicator of democratic health. Adjudications around that line are complex and should not be deputised to private companies.

23. Any determination of whether content produced by a user is illegal is a determination that may result in the removal and restriction of that content, and therefore engages that user's right to freedom of expression. On platforms that function in practice as part of the modern communications infrastructure with billions of users, such restrictions on individuals' freedom of expression should ideally not be for a private company to determine, but an independent and impartial judicial authority in accordance with due process standards of legality, necessity and legitimacy.[417] Since, in practice, companies do routinely make censorship decisions, we believe they should limit enforcement action to the standards set by human rights law whilst opening up their processes to independent audit and appeals, as discussed above.

24. Forcing internet intermediaries to accept liability for content on their platforms would likely incentivise them to be overly cautious and zealous in their approach to censoring content in order to avoid liability. It would undoubtedly result in internet platforms more actively monitoring, surveilling and censoring content on their platform at a mass scale – either by automated enforcement systems or non-judicial human moderators with extremely high workloads and limited decision-making time. These processes are not only likely to result in incorrect, inconsistent, and arbitrary decisions restricting people's right to freedom of expression, but would also lead to a generalised and persistent invasion of people's privacy. These regimes of regulation and online surveillance have a chilling effect on freedom of expression as users, knowing they are being watched and monitored online, self-censor.[418]

Q3. How effective, fair and transparent are online platforms in moderating the content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

[417] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 6 April 2018 (https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf); Article 19, 'Internet Intermediaries: Dilemma of Liability, 20 August 2013 (https://www.article19.org/wp-content/uploads/2018/02/Intermediaries_ENGLISH.pdf)

[418] https://pen-international.org/app/uploads/Surveillance-Secrecy-and-Self-Censorship-New-Digital-Freedom-Challenges-in-Turkey.pdf

Effective or fair?

25. Online platforms have not been sufficiently effective, fair or transparent in their moderation of content. There are innumerable cases of violent and plainly prohibited content remaining live, despite flagging and reporting; and innumerable cases of plainly unfair, overly zealous censorship.

26. The censorship of controversial right-wing media platform Infowars has been the first high profile example of an internet-based media outlet being virtually eliminated from common space by intermediaries, and demonstrates the deficiency in consistently effective, fair and transparent moderation. Rules had been applied to the platform sporadically and ineffectively, resulting in a public backlash that culminated in an impromptu industry-wide deplatforming after Apple delisted Infowars' podcasts. Bans by YouTube, Facebook, Twitter, Spotify, Paypal, MailChimp, Linkedin, Discus and more followed, within days. The enforcement action lacked not only effectiveness, but fairness and transparency too - despite the prevalence of misogynistic and race-baiting content, almost all of the removals were unrelated to specific posts or videos and the reasons given were generalised ones. Operators were not notified as to exactly what content was harmful or what decisions could be appealed. Critically, millions of Infowars' mostly right-wing viewers and listeners are likely to now feel a toxic combination of important and silenced – an incendiary mix. The platforms missed numerous opportunities to demonstrate they could be responsible and even-handed regulators, and finally missed an opportunity to show, with total clarity, exactly how Infowars had caused harm or breached fair rules. This alarming incident sets a dangerous precedent.

27. It is not only the enforcement of rules that is questionable, but the rules themselves. Some policies, which are rarely publicised in detail to receive close scrutiny, risk suppressing legitimate speech while allowing abuse against marginalised groups.[419] Allowing major internet companies to design and arbitrate free expression rules on their platforms has resulted in "platform law" in which "clarity consistency, accountability and remedy are elusive".[420] These platforms are enforcing systems of governance that are constantly changing, unaccountable, and opaque.[421] Platforms'

[419] ProPublica, 'Facebook's Secret Censorship Rules Protect White Men From Hate Speech But Not Black Children', 28 June 2017 (https://www.propublica.org/article/facebook-hate-speech-censorship-internal-documents-algorithms); https://www.thedailybeast.com/exclusive-rohingya-activists-say-facebook-silences-them; https://www.wired.com/story/facebooks-hate-speech-policies-censor-marginalized-users/; https://motherboard.vice.com/en_us/article/mbk7ky/leaked-facebook-neo-nazi-policies-white-supremacy-nationalism-separatism

[420] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 6 April 2018 (https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf)

[421] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2937985

moderation of content has been shown to be influenced by financial motivations, such as the threat of losing advertising[422] or losing users.[423]

28. As it stands, people's rights risk being arbitrated and even eroded by private intermediaries. It is vital that the internet intermediary companies inspire public trust and confidence in their judgments. They must take their responsibility to protect users from violent and unlawful content as seriously as their duty to uphold and promote free expression. Sensitive decisions about what is and is not permissible speech or information need to be made transparently and delivered honestly, objectively and equitably. The rules must be fair and, if they are breached, there should be clear, foreseeable consequences. Following a due process model along these lines would also mean that users would have the opportunity to appeal decisions.

29. Encouraging the major private, profit-driven internet platforms to create novel definitions for permissible and prohibited expression, and deal with the multitude of complex related issues, would allow them to set the standards by which modern society is governed and to shape the major public squares of the internet in their own moral image. That is why we believe Government should work with major intermediaries to ensure that their rules mirror international human rights law on freedom of expression and privacy, as well as UK laws, and are restricted to those standards.

Transparency

30. Internet intermediaries' policies and enforcement processes should be transparent. Some have avoided such transparency claiming that users will adapt their behaviour to evade rules. However, this is illogical and undemocratic – we do not shield criminal law from scrutiny for fear of the same. Rules must be accessible, and the consequences of breaching them should be foreseeable.

31. Intermediaries should produce comprehensive transparency reports reporting on enforcement actions, as well as Government requests for restriction and removals, whether statutory or informal requests. We welcome the initial reports of some platforms in this regard.[424]

32. Government must also be transparent. The increasing use of extra-judicial mechanisms to censor and remove content online by authorities is very concerning. Transparency reports should include details on Government takedown requests to internet platforms, via statutory

[422] https://www.facebook.com/notes/facebook-safety/controversial-harmful-and-hateful-speech-on-facebook/574430655911054; https://www.telegraph.co.uk/technology/2018/04/20/youtube-accused-still-airing-adverts-extremist-videos/

[423] https://www.telegraph.co.uk/news/uknews/crime/11392109/Twitter-boss-admits-company-sucks-at-tackling-trolls.html

[424] https://www.eff.org/who-has-your-back-2018; https://transparencyreport.google.com/?hl=en

processes as well as any other informal mechanisms. This should include information on the reasons for removal requests and the outcomes of requests.

Notification, appeal and remedies

33. Platforms should provide users with immediate notice of any enforcement action taken, as well as the reasons for the decision and information about their options, including appeals. Platforms should provide users with an appeals process to dispute enforcement actions such as content removal, restriction or user suspensions. The appeals mechanism should follow a due process model, and meaningful remedies should be available.

Q5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

34. Platforms should implement consistent, harmonised and structured processes for users – and law enforcement - to report allegedly illegal content. Platforms should improve reporting tools and the information given to users, so that these are easily and clearly available, with sufficient signposting and reporting mechanisms allowing users to report illegal content to both the platform and the police. Platforms should temporarily block the most serious content (such as threats of violence, sexual abuse imagery) pending the outcome of a formal review.

Automated content monitoring and moderation systems

35. Automated content restriction systems such as image hashing algorithms should only be used in extremely limited circumstances against narrow, clearly defined and specified content that has already been held to be illegal – for example, known child sexual abuse or terrorist content that has been prohibited through due process.[425] Any automated technology used for content moderation should be transparent, rigorously audited and subject to an appeals mechanism.

36. Academic studies have shown the difficulty with creating successful content or comment filters that can distinguish between speech that is offensive but lawful and speech that is illegal.[426] Studies have also demonstrated that automated systems are unable to understand the complexity of human language,[427] specifically "the meaning of human communication" or to "detect the intent of the speaker".[428] Even

[425] https://www.iwf.org.uk/our-services/image-hash-list

[426] Davidson, T, Warmsley, D, Macy, M, and Weber, I, 'Automated hate speech detection and the Problem of Offensive Language', 11 March 2011 (https://arxiv.org/abs/1703.04009)

[427] https://www.eff.org/files/AI-progress-metrics.html#Reading-Comprehension

[428] Duarte, N, Llanse, E, Loup, A, 'Mixed Messages? The Limits of Automated Social Media Content Analysis', 2018 (https://cdt.org/files/2017/12/FAT-conference-draft-2018.pdf)

automatic tools that scan music and video for copyright infringement at the point of upload have raised concerns of "overblocking".[429]

37. It is only appropriate to use such technology in relation to material already deemed unlawful. Automated filtering, flagging or restriction algorithms are not able to sufficiently analyse rhetorical devices such as satire, parody or irony in text or images. Such technology often results in arbitrary and incorrect restrictions of speech, rendering these tools entirely insufficient to the task of making determinations about unique content online. There should always be a human review of any unique content that is considered for restriction or removal.

Online anonymity and encryption

38. Online anonymity and encryption are key guarantors of the right to freedom of expression and opinion, and the right to a private life.[430] Anonymity allows people to express themselves freely, speak truth to power, and blow the whistle. As the former UN Special Rapporteur on Freedom of Expression, Frank La Rue, noted: "throughout history, people's willingness to engage in debate on controversial subjects in the public sphere has always been linked to possibilities for doing so anonymously."[431] Government should not unduly interfere with tools that allow people to remain anonymous online. Government should never require internet platforms to implement real-name requirements, or ID-related age verification requirements.

39. Encryption protects digital communications so that people can express themselves privately and securely. It is used to protect private communications, health data, financial transactions, and other sensitive transfers of information online.[432] Government should never require internet platforms or indeed any other communications providers to allow 'backdoor' access to encrypted communications. Government should expressly protect encryption tools.

Q4. What role should users play in establishing and maintaining online community standards for content and behaviour?

40. Users should be able to curate their own communities and environments. It would be good practice for platforms to make tools available for users to protect themselves from various categories of content, ensuring such

[429] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 6 April 2018 (https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf), page 12

[430] UN Special Rapporteur, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', 2015 (https://www.ohchr.org/EN/HRbodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc)

[431] UN Special Rapporteur, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. 16th May, A/HRC/17/27. (www.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf)

[432] https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf

tools do not restrict others' free expression. The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression advocates for user autonomy in the creation of online spaces, encouraging tools that allow users to "shape their own online environments".[433] This includes muting or blocking other users or specific kinds of content, or the use of private groups moderated by users themselves. Major internet platforms should provide the means for affinity-based groups to form given their "value in protecting opinion, expanding space for vulnerable communities and allowing the testing of controversial or unpopular ideas."[434]

October 2018

[433] https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf

[434] https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf

BPI – written evidence (IRN0081)

Response to the Communications Select Committee

1. BPI (British Recorded Music Industry) ltd. is the representative voice for the recorded music industry. Our membership comprises around 420 independent record labels and the three major record labels – Universal Music, Sony Music and Warner Music. Together, these account for more than 85 per cent of the sound recordings legally consumed in the UK every year.

Context of the current framework

2. Over the last 10 – 15 years the Recorded Music Industry has adapted to the digital age. After a long fight with piracy online, where revenues reduced substantially, consumers are turning to digital services and growth is returning to the market. Recorded music revenues rose by 10.6% in 2017, the biggest rise since 1995. Guarded optimism has returned to an industry that has faced a fight against copyright infringement as a consequence of the current regulatory framework.

3. The industry has taken a large number of actions against individual websites – 63 injunctions are in place against sites that are wholly or mainly infringing and whose business is simply to profit from criminal activity.

4. The search engines, bought to the table by Government, have started to co-operate in reducing the exposure of illegal sites in the top ranking of search pages.

5. However, all of this is in the context of a regulatory system that was set up intentionally to remove digital intermediaries from any consequences of their businesses.

6. The safe harbour in the e-commerce Directive, and transposed into UK Law, was built on the basis that intermediaries that act passively face no consequences for the activities they host.

7. This had two major consequences:

   - Firstly, it set a framework whereby doing nothing to deal with criminal behaviour or inappropriate content online unless notified by a third party was the practical way of doing business. By intervening, the defence of being a host would be diminished. Not intervening was the safest way to avoid any liabilities. As the entire system is based on third party complaints and notice and takedown, the entire burden of policing content was transferred to businesses and users. And the legal framework was ineffective – every piece of content requires a notice every time it is put up.

- Secondly, it encouraged business models that exploited the safe harbour, in preference of companies that would curate content, sell it at an economic price, and businesses that took no steps to monitor content were at a commercial advantage to those that wished to licence and intervene.

8. This has stifled innovation, and set a regulatory framework that does not act in the long term interests of consumers – that of a healthy, competitive market and one that protects consumers from harm.

9. But, put simply, it is a system that positively encourages digital providers to do nothing. The differentiation in liability between passive and active hosts means that to intervene is to create legal jeopardy. Do nothing maintains the comfy legal position of removing oneself from liability, as long as there is a system in place to respond through notice and takedown.

10. The music industry has experienced the commercial harm of a system set up to prefer free over paid content, but also the commercial burden of policing content. Sending notice after notice for the same content on the same sites. Waiting for the platforms to take the time to process the notices, and watching as people exploit the system for personal advantage.

11. We, the BPI, can fingerprint our content and crawl for it. It is expensive, time consuming and not efficient - particularly where services only need to remove the content an individual notice refers to and have no responsibility to take steps for it not to reappear.

12. This, however, is no way to cope with the tidal wave of illegal and inappropriate content on platforms and services. We cannot rely on an army of the general public spotting deliberately created disturbing content that automatically roll in playlists whilst children think they are watching their favourite cartoon.

13. The services, of course, would prefer everything to be dealt with via automation. And whilst the search engine code (see below) has shown that algorithms can help, they alone will not solve the problem. Better systems of monitoring and dealing with illegal and inappropriate content have to be put in place.

14. Online operators can and should do more to police their platforms and networks. The search round table has shown that when they co-operate, a lot can be done in a short period of time. Without the imperative to co-operate though, the current regulatory framework positively incentivises not intervening to manage harm.

15. Getting services to take greater responsibility will not stop everything getting through, and the regulatory system has to acknowledge that, but it should vastly improve the status quo. Policing of football matches does not stop every fight, but it doesn't mean we shouldn't police for the fights that it does stop.

16. At a point where the majority of 16-24 year olds are now regularly consuming their content online through services that avail themselves of the safe-harbour the regulatory system has been exposed. Content that is inappropriate, and content that is illegal, is regularly found on platforms that would not be able to remove themselves from responsibility if it were in the broadcasting regulatory regime or in physical retail.

17. The regulatory system needs to be re-balanced to ensure that the online platforms and information service providers are forced to take an appropriate level of responsibility for the harm that their platforms can create – to businesses and consumers. **Digital services should, in law, have a duty of care that will require them to be active in co-operating, and intervening where necessary, to reduce harm to consumers and to businesses.**

18. Giving the online world such a requirement to take more active steps to monitor harm and co-operate with the removal and blocking of inappropriate and illegal content from their networks and platforms will create an effective step change to reduce the criminal behaviour, inappropriate content and harm to the consumer that is rife as a result of the current framework.

Economic Context

19. **The creative industries are growing at almost twice the rate of the wider UK economy**.[435] The Creative Industries provide fantastic entertainment and support the strength of Britain's culture here and in the world, but they are also a significant economic strength for the UK. After leaving the EU, creativity will continue to be a strong export for the UK, and will be an important part of the way that the UK projects itself to the world.

20. The British music industry is a world leader. The British music industry is a world leader and has rapidly transitioned from the CD to a vast array of online and mobile services.

- Recorded music revenues rose by 10.6% in 2017, the biggest rise since 1995 with revenues of £839m;
- The increase was driven by a 45% leap in streaming subscriptions and continuing vinyl revival (up 24%);
- UK artists accounted for a 12.5% share of global sales of recorded music in 2016[436]; and
- The UK is the second largest exporter of music, after the United States.

[435] https://www.gov.uk/government/news/creative-industries-record-contribution-to-uk-economy

[436] BPI

21. Following in the footsteps of an exceptional heritage of global superstar artists, British performers still punch above their weight:

- In 2017 eight of the top 10 (and 14 of the top 20) biggest selling albums in the UK were by a British act;

- The top-selling global artist album has come from a British act in nine of the last thirteen years (2005-2017);

- The biggest selling artist globally in 2017 was Ed Sheeran;[437]

22. The outstanding creative success of the UK music industry derives from exceptionally high levels of investment in A&R (R&D) expenditure.

23. UK labels **reinvest 25% of their gross revenues in artist development** - a higher R&D ratio than the biotech, aerospace or pharmaceutical industries - and **a similar proportion again** on marketing.

24. Our business relies on copyright. The current legal framework that allows us to sell and licensing sound recordings is the fundamental right that allows our business to exist. It allows musicians and song writers to earn a living and allows record companies to make the investments they do, in the hope of a return.

25. The copyright regime, and the enforcement regime, is the most important part of the economic climate for growth in the music industry. That means being able to negotiate reasonable commercial terms for use of music by other sectors. It also means access to low cost enforcement within a strong, effective framework that means our members can protect their rights.

26. The challenge for our industry in the digital age has been to protect our rights effectively in a world where a perfect copy of our work can be uploaded shared with trivial ease.

27. In a largely unregulated online environment we and our members have had to work to protect our content and to provide services that consumers will pay for. This gives us some insight into the problems of online regulation – and the potential for Governments to take greater control.

Context of withdrawal from the EU

[437] IFPI

28. BPI is very supportive of the position of the Government that the copyright regime and the e-commerce regime is maintained post the UK withdrawal from the EU. There is certainly no appetite for yet another review of copyright, but the UK should import any appropriate measures from the current Digital Single Market process that will strengthen copyright, in particular the proposals to tackle the "Value Gap" (see below). Commitments from the UK Government on this point have been welcome as it is possible that the measures will not be in place prior to the March 2019 deadline.

29. However, the e-commerce directive also gives significant flexibility to member states to apply both legislative and non-legislative measures to tackle illegal and inappropriate content. The UK could apply greater enforcement measures and require greater co-operation from intermediaries through codes of conduct.

30. The measures proposed in this submission are all possible under the current framework, and indeed might pre-empt the EU's own review of the effectiveness of online enforcement.

31. **The UK could, and should, prioritise modernisation of its own legal framework for online enforcement** to drive the next stage of growth online – making the UK a world leading market for certainty for legal services and content creators and greatly improving the confidence of consumers in the experience and legality of online services.

Online regulatory framework - The Value Gap

32. The biggest single barrier to growth in the music sector is the distortions in the digital economy that undervalue music compared to the consumption and revenues of some of the digital platforms that exploit it. This is revenue that can be reinvested in a greater pool of artists, increasing our ability to compete and grow in the global competition for listening. This is what BPI calls "the value gap".

33. The UK has led the way in developing legal services. In 2017 there were 62.5bn audio streams and 'at least' 25bn video streams (our data from video streaming services is not complete). Audio streams grew at a rate of 50% in 2017 and is set to power a sustained period of growth for the UK music industry.

34. The innovation in the services licensed by BPI members allows consumers access to nearly 40 million tracks through music services such as Apple Music, Spotify, Deezer and Google Play. Consumers can download, stream, and listen to music offline on services that are portable wherever they are in the world and convenient to use.

35. However, in competition with these licenced services there are certain online services such as YouTube, DailyMotion and SoundCloud which allow users to upload content themselves. These services feature such "user generated content" but also host and distribute a huge volume of professionally-produced entertainment content including official music videos or recordings by commercially successful recording artists.

36. This professional copyright content is enormously popular and plays a major role in driving the growth of these platforms. N**ine of the top ten most watched videos on YouTube are official music videos by artists such as Louis Fonsi, Ed Sheeran and Justin Bieber**.

37. Because these services allow users to upload content, they claim the benefit of loopholes in copyright law – called "safe harbours" – which give immunity from copyright liability to services which host user uploaded content, provided they respond to "takedown notices".

38. These "safe harbours" were put in place more than fifteen years ago to protect passive hosting services, and were not intended to protect sites which build their services around facilitating access to music and maximising revenue from the availability of music, which have become the number one means to access music amongst key demographics.

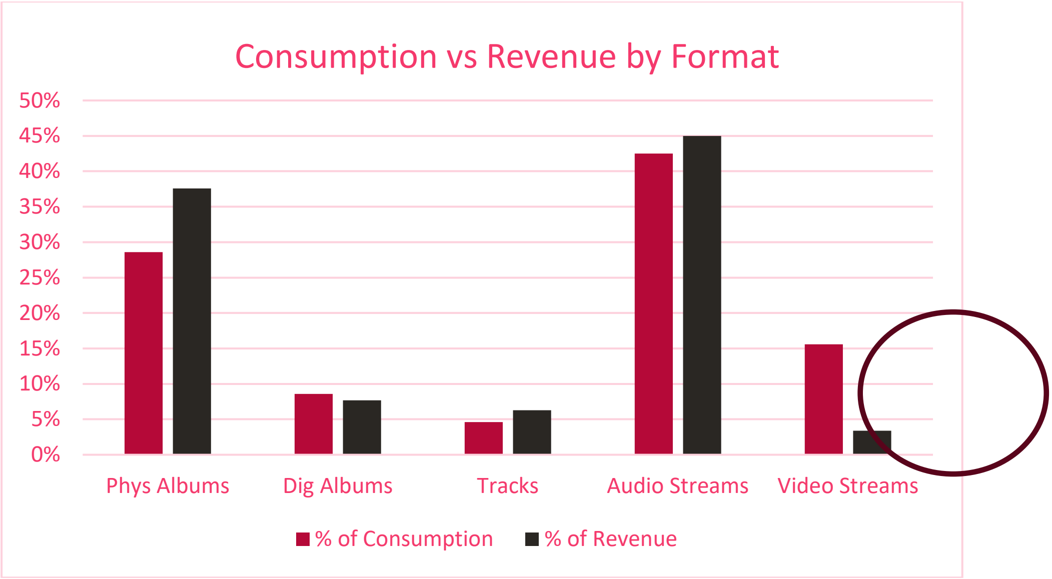
39. Understandably, policy makers at the time could not possibly have anticipated the wide variety of digital services and business models that would be developed in the years to come but they might have considered that the principle was open to abuse.

40. Major music services such as YouTube now hide behind the "safe harbour" provisions arguing that their users are making available copyright content while they themselves are nothing but mere passive intermediaries.

41. This leads to licences being concluded at artificially low rates, causing a huge "value gap" between the rates paid by such services for their use of music, and the revenues returned to labels and artists from other services such as Spotify and Apple Music, which are licensed on arms' length terms. As a consequence in the UK, vinyl sales generate twice as much income to the recorded music industry than YouTube does.

42. **The number of streams, both audio and video, have been increasing significantly in recent years as consumption has moved online.** Users use YouTube as they would a music streaming service – using it to locate their favourite songs and listen to their favourite artists on-demand.

43. However, whilst consumption of both audio streams and video streams have grown, a significant gap has opened up in the value those differing services return to music companies and artists. This is shown below.



44. The main facts are that:

- Video streaming services (of which YouTube is by some distance the dominant one) contributed a meagre 3%, just £27.1m to overall revenues, in 2017 despite accounting for an estimated 16% of consumption.

- This stands in stark contrast to the £346.9 million that audio streaming services (such as Apple, Spotify and Deezer), contributed to artists and labels from a similar number of streams –five times as much per stream; and

- The £27.1m generated by video streaming – principally music videos streamed on YouTube – **contributed around half of that of vinyl sales to the recorded music industry in 2017.** Vinyl represented £55.1 million of earnings.

45. This is the **"value gap"** – the gap between the consumption of music videos and the revenues earnt - and it is caused by UGC platforms relying on copyright loophole "safe harbours" in EU legislation to pay much lower royalties than competing services.

46. In reality, the activities of these Services often go beyond the mere provision of hosting services, because the operators get actively involved in the presentation, arrangement, usage and distribution of the content to the point where they themselves are making content available to the public.

47. The UK has announced its intention that it will translate current EU directives **and the Aquis** into UK law. Under the existing European and international copyright framework - the WIPO treaties on which the Copyright Directive is based - and CJEU case law, providing "access" to works is covered by the communication to the public right, unless the activity amounts to nothing more than the provision of physical facilities (so, for instance, merely providing a public address system to a shop would not amount to communication to the public by the provider of the hardware).

48. The fact that content is supplied by users does not exonerate User Generated Content services such as YouTube from copyright liability. This has been confirmed by the CJEU,[438] in particular in cases where the public would not have had access to the content without the service's deliberate actions, which is the case with UUC services.

49. It follows that under the criteria developed by the CJEU providing public access to content uploaded by users of a service is an act of communication to the public, restricted by copyright, and user generated services are engaging in that act.

50. However, as the text of the proposed Commission "Recital 38" states, the fact that services engage in a restricted act does not mean that such services would in every case be liable for copyright infringement and therefore required to obtain a licence. It is possible that a UGC service that communicates (or makes available) content to the public is eligible for the safe harbour for hosting service providers under the E-Commerce Directive.

51. It is important to note that clarifying liability would not have a negative effect on the availability of user generated content. UGC is widely available thanks to right holders' licensing practices, which right holders will continue with.

52. This **clarification would eliminate a major distortion in the market for content** which is benefitting major US tech platforms at the cost of UK creators. It is urgently required if we are to maximise growth from the UK digital economy and to ensure that artists can earn a fair return from their work in the digital era. It is, for the music industry.

53. The UK Government has been supportive, and this is the single most important measure it could take – by bringing into domestic law - to speed up growth in the sector.

Enforcing copyright to increase investment and growth

54. The UK has led the way in developing legal services. Consumers can access a vast history of licensed, legal music – for free, in most cases, through ad funded services such as YouTube or Spotify free tier.

[438] See e.g. SBS, C-325/14; Airfield, C-431/09.

55. The innovation in the services licensed by BPI members allows consumers access to nearly 40 million tracks through music services such as Apple Music, Spotify, Deezer and Google Play. Consumers can download, stream, and listen to music offline on services that are portable wherever they are in the world and convenient to use.

56. Since July 2015 the music industry has a "global release day" where record labels release new music to almost every territory in the world on the same day, Friday, and it is instantly accessible to consumers through the vast array of digital services.

57. At the same time BPI recommends to its members that they follow the principle of "on air, on sale" - if you can listen to a piece of music on the radio or on a digital service, you should also be able to purchase it for individual consumption.

58. Music has provided every kind of digital service to access music legally, often for free, through licensed services that give money back to the people that make that music – artists, songwriters, performers and the investors that publish and fund the production of music.

59. Yet piracy is still a large problem for all of the Creative Industries. Based on the IPO tracker survey and average retail prices, from academic evidence of replacement rates BPI estimates that the **losses from piracy to the UK recorded music industry are between £150m and £300m a year**. This is a significant loss of value to the UK economy, to taxation and to legitimate businesses in the whole of the value chain, from retail to production.

60. The business model of illegal sites and services is often directly or indirectly supported by intermediaries such as search engines, advertisers, payment service providers, mobile app store operators and domain name registrars. Some progress has been made with voluntary solutions in some areas, advertising and payment providers and the work with ISPs on the *"Get it Right from a Genuine Site"* campaign; however more could be done to effectively address the problem of intermediaries being embroiled in unlawful activities and to give intermediaries appropriate incentives to act.

61. BPI believes businesses operating online should co-operate willingly to drive out illegal companies and ensure that consumers have a better, safer online experience. We welcome voluntary arrangements that have been put in place with the online advertising industry and payment providers, with work co-ordinated by the Police Intellectual Property Crime Unit and the use of an independently verified Internet Watch List of illegal sites to help bear down on their sources of income.

62. One of the important measures the UK has taken has been the voluntary code of practice on responsible search. **The voluntary code of practice signed by Google and Microsoft Bing together with rights holders was a world first.**

63. The code has ensured that there is collaboration between the parties to demote links to websites that are dedicated to infringing content for consumers in the UK. It is only collaboration that can lead to a long term solution and already it has shown itself to be successful, with Google for instance making algorithm changes to remove illegal sites from the top pages of listing, and doing so worldwide.

Greater co-operation and engagement from digital services

64. The UK's pioneering approach with the Search Code of Practice, which the Government facilitated last year, led directly to a global change in Google's algorithm so that illegal sites are demoted out of search results much more quickly. Our colleagues in the rest of the world have now seen the results of the UK process in their own country search results. This generates further benefits by improving the return to the UK from overseas markets.

65. Whilst the UK does have relatively high standards of enforcement compared to the rest of the world, it should keep pressing ahead and making it easier for legitimate businesses to grow and harder for illegal sites to siphon value out of the UK creative industries.

66. Government can, through the Digital Charter process, make a real difference by taking bolder steps. There are two specific aspects where the UK could take legislative powers that could represent the next leap forward in legitimising the online marketplace in the UK:

1) Administrative site blocking

67. BPI and others have shown that site blocking is effective and has a significant impact in reducing piracy. BPI has brought High Court actions blocking 63 major illegal sites in the UK, which has starved them of traffic and advertising revenues. However, it is still extremely expensive and time consuming to bring a case, which means that such court actions are suitable to deal only with the largest illegal sites and are accessible only for more significant organisations such as BPI.

68. The Digital Economy Act 2017 introduced administrative site blocking for sites that host sexual content but do not apply effective age filters. This has been accepted by the general public as an appropriate step to take.

69. The UK should extend the principle of administrative site blocking to copyright infringement, allowing for a regulator to produce guidance on evidence required, with a clear process and built-in checks and balances for intermediaries, including of course the possibility of judicial review. The process could be available for sites that are mainly or wholly infringing and provide a much faster mechanism to prevent illegal sites from exploiting the substantial delay in action being taken that results from the costs and administrative burden of the High Court system.

70. This approach has been taken in some other countries[439], with Italy's administrator AGCOM leading the way, set up via a regulation adopted in 2013. From its launch up to April 2017, AGCOM had received 729 complaints; out of which 424 had been processed by the authority and 277 ended with the blocking of access to a website, of which nearly 100 are music sites. This is a significantly faster and more effective process than a court process, and can deal with a much greater volume.

71. **In addition, Government could take powers within this system to place obligations on other intermediaries not to facilitate the sites that are blocked** – including removing links in search to proxy sites seeking to circumvent the block and requirements on UK advertisers to take reasonable steps to remove adverts from such sites.

2) Notice and Staydown

72. The notice and takedown system of copyright enforcement created under the US Digital Millenium Copyright Act 1998 (and adopted widely in Europe as a means of complying with the EU e-commerce directive) was designed in an era when content available on the internet was expected to be principally legitimate. It was designed as a reactive system to deal with a small percentage of illegal files hosted on essentially legal platforms. The DMCA did not foresee the explosion of blatantly illegal websites or the emergence of hosting sites, funded by advertising or subscription, whose business models rely almost entirely on making available large libraries of illegal content for free.

73. Notice and take down was not intended as, and is not fit for purpose as, a mechanism to remove vast amounts of infringing content from services that benefit financially from the content and actively curate it.

74. Illegal services hide behind published "notice and take down" policies so as to take advantage of safe harbour protection under the DMCA and the e-commerce directive, structuring their business so as to exploit the benefit of the period between the upload of an illegal file, its posting detection by right holders and the receipt of a notice requiring that URL's specific removal.

75. The legal framework has not kept pace with advancements in technology that mean that is simple and cost-effective to screen hosted content using file-hashing or fingerprinting technology so as to prevent illegal content which has already been the subject of a valid takedown notice simply being re-uploaded.

[439] Administrative site blocking exists in Italy, Spain, Mexico, South Korea, Malaysia and Indonesia. Last year, Greece also adopted legislation introducing an administrative procedure.

76. A high proportion of the takedown notices sent by rights holders are repeat notices for the same content on the same sites. IFPI, the (International Federation of the Phonographic Industry) measures the five largest cyberlockers, UUC, and referrer sites and, in 2014 IFPI found that 94% of the notices sent over the course of a year were for content for which IFPI had already sent a previous notice. By 2016 this had risen to 96%.

77. BPI's own analysis of the notices sent on behalf of music companies to the top 5 most infringing lockers, UUC and mp3 sites showed that within a 4 week period, BPI sent notices for the removal of Adele's Hello from one of those fifteen services 2258 times.

78. This demonstrates that there are a vast number of notices that, once complied with, only lead to the same track being reposted almost immediately on the same services; despite the fact that the hosting service is fully aware, once a notice has been received, that it has no legal right to list or host that track.

79. Advances in technology mean that it would be appropriate and proportionate to require hosting services to operate a system of "notice and stay down", whereby once a specific infringing file has been notified to a service provider, that service provider must take reasonable steps to ensure that all other copies of, or URL links to the same copyright content (a) are also removed; and (b) do not appear on their service in the future.

80. A strengthened enforcement regime would both increase the value of the UK creative Industries and, as a consequence, increase investment into the sector, creating a multiplier effect across the economy. The measures proposed above would have a strong positive effect on the already rapidly growing UK creative economy. They would also make the UK enforcement framework more accessible and effective for small business rights owners, promoting stronger growth in the crucial SME sector of the creative industries.

Education on copyright and legal services – Get it Right from a Genuine Site

81. BPI is also conscious that industry can help to educate the public, to turn people away from the pirate enterprises and help to reduce the effectiveness of criminal online behaviour. If we can help move consumers to legal services, the burden on the legal process should also be reduced as the criminal behaviour is reduced.

82. BPI, together with the MPAA, has been working with the Government on a copyright education campaign, *"Get it Right from a Genuine Site",* to highlight the importance of respect for copyright. New creative content requires the significant investment that copyright allows.

83. The campaign has been built with considerable investment from the movie and music industries, supported with £3.5m of Government money. As such it is a great example of partnership, and the management of the campaign by the industry itself has allowed it to work flexibly and ensure it is relevant to the sector it covers

84. Most importantly, it has shown very positive results, according to independent research undertaken to monitor its impact.

- IPSOS polling in Dec 2016 showed **26% of people have been exposed to the campaign** – 1 in 4 people – in the 16-50 age group targeted.

- **Amongst those exposed to the campaign**, **past month piracy rates have fallen by 18%** - from 57% in Dec 2015 to 47% in Dec 2016. For the public in general piracy rates have remained constant.

- Those exposed to the campaign are more likely to think it is worth paying to safeguard creative industries - 79% of the exposed versus 67% of the general public.

- And the exposed are more likely to feel accessing pirated content is unfair to content creators - 68% compared to 63%.

May 2018

Brass Horn Communications – written evidence (IRN0044)

This submission is written on behalf of Brass Horn Communications, a small non-profit Internet Service Provider based in the United Kingdom.

Background:

Brass Horn Communications specialises in providing censorship and surveillance resistant Internet services to the global community.

We are greatly concerned that the language of "regulating the Internet" in an effort to tackle 'fake news' and abusive messaging belies the dangers of damaging the infrastructure that empowers the global free exchange of ideas.

We must be very careful not to conflate the Internet *(the infrastructure)* with the online platforms/"Internet Giants"/Social Media companies that operate on top of it.

The UK Government should not attempt to interfere with the technical operation of the Internet infrastructure and instead leave the regulation of the Internet infrastructure to the global multi-stakeholder community.

1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

The Internet is by definition an inter-connected set of independent networks, any legislation or regulation passed would only apply to the UK. For the Internet to remain global the UK networks would be required to stay connected to networks in other parts of the world and these networks would not necessarily follow UK law rendering the regulations ineffective.

Applying regulation to Internet infrastructure at national boundaries has been widely decried as Internet Balkanisation *(including by the UK Government440)* and would detrimentally impact UK Internet businesses whilst at the same time be unlikely to achieve the stated aims.

The Internet is a special medium, many see it as a form of media consumption, but unlike TV or Radio it is by design a two-way system. When you tune into BBC1 on your TV it is picking out a small slice of the received TV signal being broadcast, the Internet however requires your computer to send information to BBC.com and then BBC.com sends information back.

If information can be sent from an individual computer to the Internet then that computer can be a publisher as easily as it is a consumer. This is the power of the Internet. Any computer can be a online platform, even a mobile phone can be the server for a small blog – this makes regulation of publishing content difficult as any device capable of being a receiver is at the same time a broadcaster.

[440] https://techcrunch.com/2017/08/24/we-dont-want-a-balkanized-internet-says-brexiting-uk/

Unlike roads or radio frequencies the global community decided that the Internet was a medium that everyone could use without a license or permission and it is this permissive environment that has made it such a success. Attempting to constrain the Internet *(the infrastructure itself)* would damage digital innovation in the UK but ultimately be ineffective at preventing people misusing it.

We would encourage the committee to experiment with asking if it is possible to regulate the road or pavements to prevent the spread of hate speech or fake news. One could pass laws that say people cannot use a road or pavement to transport flyers or newspapers that contain fake news or hate speech but how would the Police enforce this without a draconian approach such as blanket stop and search?

Would searching every vehicle on the road or every pedestrian be proportionate? Would it be effective? Would people change their message or start to use code? Would they transport blank paper from point A to point B and then print their fake news / hate material at the end of their journey?

Many advocates of Internet regulation point to BT CleanFeed and the IWF as models of regulating the Internet, we would put forward that CleanFeed has become a tool of censorship and is *possibly* no longer effective for its original purpose *(e.g. it cannot stop access to illegal material published on private channels or within messaging apps).*

In 2004 Bill Thompson, a BBC commentator on Digital Issues, warned[441] that CleanFeed could be used for other forms of censorship. It only took a few years till we saw the Honourable Justice Arnold order websites that weren't technically illegal be blocked using the CleanFeed system, his stated reason for ordering the blocks can be summed up as *the system for blocking websites existed*.

The IWF has a noble goal but as with any approach that utilises censorship it has made mistakes. This has caused the temporary loss of Wikipedia and other notable websites – the IWF lists are secret *(for obvious reasons)* but this is problematic from a transparency viewpoint.

The evolution of CleanFeed is the so-called ISP "Family Filters" – these filters have been found to erroneously block ChildLine, the NSPCC, the Samaritans and many more websites.[442] Websites that adults and children alike may have needed in times of crisis only to find that they have been blocked "for their safety", this is unacceptable.

The opportunity for misuse of any regulation that aims to constrain the Internet is too dangerous to be allowed and would possibly violate EU law[443]

[441] http://news.bbc.co.uk/1/hi/technology/3797563.stm

[442] https://www.openrightsgroup.org/press/releases/orgs-blocked-project-finds-almost-1-in-5-sites-are-blocked-by-filters

[443] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2017-005328+0+DOC+XML+V0//EN&language=en / http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2017-005328&language=EN

The Windrush issues, the Undercover Policing Inquiry and the Snowden revelations show that Governments cannot always be trusted with certain powers. The Internet is the greatest innovation for collaboration, empowerment and communication humankind has ever seen – we cannot allow the Government of a supposedly free and open society the power to strangle the underlying infrastructure.

To answer whether regulation is possible the short answer is; not effectively.

Brass Horn Communications specialises in defeating Internet censorship both here in the UK and abroad. We build new technology and help empower existing technology to ensure that the Internet continues to work as originally envisaged, that is to say; a packet of data can travel from point A to point B and back again reliably and securely.

We would encourage the committee to read the "Declaration of the Independence of CyberSpace"[444] as this may help to understand why some of us in the Internet community resist the idea of Government regulation of the *infrastructure*. Once a Government starts to exercise regulation in the form of censorship *(fake news, hate speech, etc)* then it is difficult to stop the state adding new categories to the list. Russia, China, Iran and other countries seek to "regulate" the Internet through censorship – the UK should not be part of this group.

Sending abusive messages has been illegal since 1988, glorifying terrorist/extremist content is illegal, hate speech is illegal – to return to the pavement analogy; just because people are using the Internet instead of soapbox in the street doesn't change that **their** behaviour is illegal – pursue the criminals, don't criminalise the company that laid the paving slabs.

Internet intermediaries should not be regulated in a drive to control content – we need to ensure that a packet of data sent from a users computer gets to its destination and the reply from the destination gets back to the users computer. Without this guarantee the Internet will be fundamentally broken.

2. What should the legal liability of online platforms be for the content that they host?

In Internet technology communities it is usually understood what we mean when we discuss volume of content to be on a "human scale" or on a "Facebook scale".

Newspapers, Television and other mediums operate at human scale, there are a few content creators who report to a sub-editor and those sub-editors report to an editor or program director etc.

The companies in question have a political leaning, a stated editorial goal and everyone works towards that goal.

[444] https://www.eff.org/cyberspace-independence

A few hundred people might report into a handful of people who in turn report to a yet smaller group of people.

Teachers marking homework is human scale.

MPs holding surgeries with constituents is human scale.

Online platforms harness the creative output of the **global** population – the variety and scale of this output is difficult to measure and borderline impossible to pro-actively police.

Are we asking if the owners of Wembley stadium should be liable for what one, two or even one hundred people in a crowd of tens of thousands chant or a placard they hold up? Even if we did, the scale of Wembley stadium is still nothing compared to the number of messages, hours of video and gigabytes of images uploaded to the large platforms *every second of every day.*

By making online platforms liable for content they will respond by censoring on the side of caution, this will affect marginalised communities and legitimate political speech. This is dangerous for a free and open society as people will be silenced, they might even get isolated from friends and family if their account is erroneously banned[445] by a mistaken categorisation. An excellent example of this is the US FOSTA/SESTA legislation which has resulted in mass deletion of entire online communities.

Many advocates of holding platforms liable will point to the IWF takedown statistics or Microsoft's PhotoDNA product as exemplars of how "it can be done if the Internet giants want to" but again we've seen issues with false positives.

A notable recent incident is one where Facebook deleted the iconic photo of Kim Phúc in 2016[446] due to systems put in place at the request of Governments, this was widely acknowledged as unacceptable and a mistake – but only because it was a newspaper with a global audience that was impacted. What impact or recourse would an individual have had?

Advocates of such technology are happy for false positives to occur.

In support of this claim we make reference to the Children's Charities' Coalition on Internet Safety – written evidence (IRN0008), in which they applaud CleanFeed and PhotoDNA without the need for an independent audit but claim that without an auditor they could not be confident that the moderation policies of online platforms were fair and effective.

These methods are used by more restrictive Governments to control freedom of speech in their countries; in Vietnam there are concerns that Facebook is silencing political activists using similar systems[447] of censorship.

[445] https://themighty.com/2018/03/twitter-reporting-suicidal-tweets/

[446] https://www.theguardian.com/technology/2016/sep/08/facebook-mark-zuckerberg-napalm-girl-photo-vietnam-war

[447] https://www.reuters.com/article/us-facebook-privacy-vietnam/vietnam-activists-question-facebook-on-suppressing-dissent-idUSKBN1HH0DO

Returning to question 1, if a person knew that anything they wrote on a UK affiliated online platform could result in censorship they might opt to use a different platform. The regulation would be nullified and the content would remain published. The only entities losing out are the UK businesses that people wouldn't trust.

It is bad enough that UK infrastructure cannot be trusted to be free of "backdoors" due to the Investigatory Powers Act but adding onerous censorship as well would be even worse.

Because of increased censorship *(and surveillance capitalism)* we are already seeing a move to decentralised technologies such as Mastodon448 and MaidSafe449 – with these technologies the user is the online platform. There is no one company that can be held liable for the content, the only person who can remove the content is the user who published it – by forcing regulation upon certain companies the Government may inadvertently make the situation less controllable.

Online platforms should not be held liable for their users content for several reasons;

- Those that err on the side of caution will inevitably censor marginalised communities
- It will adversely affect smaller platforms that can't develop or buy the technology / resources required to monitor content
- Active monitoring of content will result in a chilling effect on users
- We will possibly see a withdrawal from the UK of certain providers *(which will still be accessible to UK citizens due to the global nature of the Internet)*

11 May 2018

[448] https://mastodon.social/about
[449] https://www.maidsafe.net/

Bristol Safeguarding Children’s Board - E-Safety Working Group - written evidence (IRN0009)

Evidence provided and submitted by the Bristol Safeguarding Children’s Board – E-Safety Working Group. This group is made up of teachers, school staff, local authority safeguarding experts, voluntary sector organisations and representatives from Avon and Somerset Police. The remit of the group is to promote excellent practice with regards to e-safety across the city, disseminate information from the board that is relevant to our specific area of expertise and advise schools on how to meet their obligations with regards to e-safety.

Question 1 - Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

The Bristol Safeguarding Children’s Board – E-Safety Working Group believe that regulation of the internet is desirable up to a point. The reason that we say ‘up to a point’ is so that we can still respect the right of free speech and free information without the state interfering and limiting what it’s citizens can access. We also believe that it would be quite difficult to regulate the internet as it is a global resource and depending on the regulation, companies or sites would be able to move where their site or resource is located to avoid having to comply with regulation.

The Group believe that it may be better to regulate access to content as too many children have access to inappropriate and dangerous content. This could be done with new legislation or by tightening up current legislation.

There is also a danger of doing nothing as this could portray to those who need regulating that legislation and regulation have been given up on.

Question 2 - What should the legal liability of online platforms be for the content that they host?

There is a responsibility on website hosts to moderate the content that they are hosting. It should be appreciated that this job is particularly difficult as the nature of the content the moderators are viewing is likely to be distressing. Companies should be required to put in place supervision for their employees to ensure that they are being looked after. Any regulation should insist that moderators are employed by any company that host internet traffic and content and that they are looked after. Terms and conditions could also be strengthened so that any illegal content that is posted by a user will automatically be reported to the police.

The Group find it remarkable that illegal activity or content can be posted onto a site without any comeback on the host. Therefore, the legal liability should be held with the online platform to remove the content and report the user who posted it to the police.

Question 3 - How effective, fair and transparent are online platforms in moderating content that they host? What processes should be

implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

Effective, fair and transparent mean extremely different things. Taken to mean that online platforms operate as they are expected to, generally they are only effective if content breaks their own terms and conditions. Generally, the Group believe that online platforms are not transparent as the user does not tend to get reasons for the removal or non-removal of content that has been reported.

The process for individuals who wish to request the decision to be reversed could be done by an ombudsman of some description, however it seems unlikely to be effective as the content would only be removed if it broke the terms and conditions that the user agreed to when they signed up to site. It would therefore make more sense for any regulation to insist that companies publish the reason for their decision when it comes to removing or not removing content, for each company to have an escalation policy internally and for the terms and conditions to be stronger when it comes to illegal content or bullying behaviour.

Question 4 - What role should users play in establishing and maintaining online community standards for content and behaviour?

Users have an extremely important role in establishing and maintaining standards because they are likely to become aware of content before the site that is hosting it. The Group believe that the terms and conditions of any site should require users to report content, and that if the site becomes aware that a user has viewed content without reporting it there should be some sort of comeback such as not being able to use their account for a period of time.

It is also important to ensure our young people know that it is part of their duty as a citizen to report content and behaviour so as to protect others. This means that our education providers will play an important part in getting this message across.

Sites that host content should also make it easier to report content. For example, if you can 'like' a photo or comment with one click, then you should also be able to report a photo or comment with one click. The reporting process can often be long-winded confusing (if you have to choose a category) and depending on choices that are made as part of this process, reporting can't actually be done. If reporting is simple and efficient to do, it is likely that more people will do so.

Question 5 - What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

As default, online platforms should ensure that privacy settings are set to the most private setting possible to protect information that users submit. They should also ensure that all information stored on company servers is encrypted so that if a breach does ever occur, the information is useless to those who have gained access.

Information that is submitted as part of a sign-up process should be strictly limited to what the online platform actually need to know. This should be happening now as part of the change to the GDPR and the new Data Protection Act.

Question 6 - What information should online platforms provide to users about the use of their personal data?

Online platforms should provide users with a short, 1 page summary of what they do with the data that any user submits. This should be bullet-pointed and in clear and easy to understand language. This should be being done already as part of the GDPR.

Question 7 - In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

If a regulator was to be set up, they could insist that all algorithms that are used are sent to them for review or approval first. This way, anything inappropriate or which breaches the GDPR or other legislation can then be challenged.

Question 8 - What is the impact of the dominance of a small number of online platforms in certain online markets?

The impact of the dominance a small number of online platforms have is huge as it comes across that they feel like they can do whatever they want. By being predominantly self-regulated, they have also had the opportunity to dictate the rules to governments and be judge, jury and executioner in all cases.

It is also remarkable to think about how much data they hold about citizens of any country which has been freely given to them. It isn’t hard to believe that there is a high likelihood that online platforms know more about people than their government. Considering the amount of fuss made when governments try to know more about their citizens for legitimate reasons (such as security), the very same people hand over even more data to online platforms. This also means that these platforms know a lot about our young people which could have a serious impact on their lives in the future – we don’t know this yet as the generation who have grown up with technology are only just reaching the stage where they are looking to take the next step in their lives.

The benefit of only a small number of platforms being dominant is that it may be easier to affect change as only a small number of companies need to be involved.

Question 9 - What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

The United Kingdom leaving the European Union will affect the ability of the UK to regulate the internet as we will no longer be able to negotiate with these very powerful online platforms as a bloc to effect change. It is more likely that online platforms will listen to governments or organisations who have the most users or where everyone is saying the same thing.

Remembering that the internet is truly global, investigations that involve countries within the EU will need to be able to happen so that criminals who use the internet are brought to justice.

If the UK Government is hoping to be a world leader on internet regulation, then we need to be assured that we are still able to influence other governments and global organisations. It is not immediately obvious what the other vehicles are to ensure our voice is heard – the European Union seems the most likely and most able to rapidly effect change in this area, especially considering the work they have done with data protection.

3 May 2018

British and Irish Legal Education and Technology Association (BILETA) – written evidence (IRN0029)

Summary of Response

1. The internet is too complex for a single regulatory framework. We, therefore, suggest that the current laws and regulations are kept in line with the EU laws and developed for the benefit of the open Internet, driven by human and user rights.

2. The legal liability of online platforms, remains quite low based on Article 15 of the E-Commerce Directive. This is further supported by a growing body of legal scholarship which indicates that online platforms should not be required to proactively monitor, filter and block content uploaded by their users. There is also the argument that notice and staydown measures could be incompatible with both the EU Charter and CJEU/ECtHR case law.

3. Whilst online platforms reflect efficiency in moderating content they host, the procedures in relation to transparency and fairness can be improved, particularly, in relation to appeal processes and complaints mechanisms. In this sense, the UK can also learn from the US (DMCA 1998) and some EU countries where users are notified of takedowns requests and are given the opportunity to send counter-notices reflecting 'put-back' processes.

4. In the context of users, it must be recognised that online communities whilst sharing some key characteristics with offline communities are fundamentally different in their composition, and in what is deemed as acceptable behaviour. The Internet Safety Strategy document sets out the Government's intent to improve safety online; however, simply imposing a code of conduct on online communities will not satisfy this desire. Involving users in establishing and maintaining community standards is a way forward.

5. Freedom of expression (FoE) and freedom of information (FoI) are two very important rights, which needs to be protected online although they are not the only two online rights – all rights ought to be protected. Platforms need to balance FoE rights whilst maintaining standards for content, behavior and participation rights.

6. Platforms should be attentive in relation to providing information to users as required by the GDPR 2016 and the Data Protection Bill 2017 thereby abiding by the principles of transparency and accountability. It is also essential that platforms provide information regarding the use of the deceased's data, which is currently lacking.

7. It is imperative that platforms clearly explain their business models and the manner in which they use personal data of their users, as well as the effect the processing involving algorithms can have/has on individuals. If their business model is not based on using personal data for advertising, it should still be set out in clear terms.

8. The ‘Big Four’ – Google, Amazon, Facebook and Apple (GAFA) will continue to have powerful influence on the way we work and live. Yet, it is not the GAFAs one should be concerned about. China’s internet giants Baidu, Alibaba and Tencent (the BATs) are now taking the lead and regulation in this area will need to go beyond competition law.

9. UK’s departure from the European Union raises various questions on regulation as well as deregulation. However, the confirmation that the Charter of Fundamental Rights of the European Union 2000 will be retained in UK domestic legislation after Brexit, will mean that equivalence, adequacy or compatibility of UK law will be assessed by the European Commission in view of the interpretation of UK law by the CJEU after Brexit – which is a step forward.

1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

1. The internet is too complex for a single regulatory framework, as it includes the infrastructure (regulated by telecoms law and policy), standards and protocols (regulated by organisations such as the Internet Engineering Task Force, W3C and ICANN) and content (regulated at a national level, e.g. privacy, e-commerce, libel, criminal and intellectual property laws). These terms should not be confused and the focus of this inquiry should be on the regulation of content, platforms (intermediaries as they are commonly known in our scholarship), and some aspects of telecommunications law.

2. We acknowledge that the current drive to regulate the internet comes from data and ad-driven platforms with market dominance, mainly American, and being perceived as powerful enough to affect and manipulate the democratic process. Some of the issues we have seen recently, e.g. Cambridge Analytica and the US elections, relate to very different areas of law, such as electoral laws, privacy and access to information. These concerns should not result in the entire complex structure of the Internet being regulated as one entity.

3. We support the principle that "the same rules apply online and offline", but we also note that rules need to be applied in a way that takes into account the implications of technology.

4. One of the key problems is that the Internet mainly consists of private infrastructure, therefore a lot of regulatory interventions works through private companies. These companies and platforms have to make decisions about user rights, they interpret and enforce the law and courts are seen as the last resort (e.g. privacy, copyright or libel).

5. We also note that there have been numerous problems with self-regulation, especially in the area of privacy and data protection (e.g. cookies and online advertising witnessed a complete failure of industry self-regulation).

6. We, therefore, suggest that the current laws and regulations are kept in line with the EU laws, and further developed for the benefit of the open Internet, driven by human and user rights.

2. What should the legal liability of online platforms be for the content that they host?

1. Laws such as libel, intellectual property and e-commerce provides provisions for liability for online platforms hosting infringing content or in violation of human or private rights. For example, the *Defamation Act 2013* (extending to England and Wales only) requires that an online platform removes infringing material when notified or requires that the website will cease to distribute, sell or exhibit material. However, this requirement becomes active following a court judgement.

2. Such provisions also exist under intellectual property laws, where following a court judgement, the infringer will be required to cease operating or host counterfeit or pirated content.
3. However, the *Defamation Act 2013* provides a defence to online platforms which can establish that it was not they who posted the comment or content. The defence is defeated if the online platform had notice of the content and was slow to respond.

4. Similarly, most online platforms will benefit from Articles 12-15 of E-Commerce Directive[450] which provides a safe harbor provision to internet intermediaries such as, hosting services platforms by offering them immunity from liability. One of the conditions for such immunity is that under Article 14 of the E-Commerce Directive intermediaries act "expeditiously to remove or to disable the information" upon obtaining the knowledge of infringement. This provides a legal base for the widely adopted practice of "notice and take down". In other words, when a person identifies an infringement of their rights – whether it be a violation of human rights (e.g. privacy) or violation of their private rights such as intellectual property laws (e.g. copyright, trade marks), the relevant person can notify the intermediaries requesting that they take down the infringing information from their platforms.

5. Whilst this appears to be an efficient mechanism, it does not always work as well in practice. In most cases, the content is removed *after the harm* has occurred. On the other hand, the use of ''notice and staydown'' measures, which involve the real time monitoring, filtering and blocking of user uploaded content can easily lead to mistakes, specifically the blocking of lawful content (false positives) or the passage of unlawful material (false negatives).

6. What is controversial is regarding how the internet intermediaries should *acquire knowledge* of illegal activity or information. At the moment, the burden on online platforms is quite low and this is in part due to Article 15 of the E-Commerce Directive, which sets out that online platforms have no general obligation to monitor all the activities which take place on their platforms. For example, in a recent case concerning *Google* the court ruled that a search engine is not expected to monitor all the activities of all their users[451]. Moreover, in *Sabam v Scarlet*[452] *Sabam v Netlog*[453] and *Mc Fadden*[454] the CJEU found that notice and staydown measures, which involved the real time monitoring, filtering and blocking of user uploaded content failed to strike the right balance between, on the one hand, rightholders' rights, and on the other, internet intermediaries and users' rights. The use of unregulated private sector surveillance and censorship of information would also be incompatible with the ECtHR case-law -

[450] E-Commerce Directive, 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

[451] Case 236/08 *Google France, Google Inc. v Louis Vuitton Malletier;* Case 237/08) *Google France SARL v Viaticum SA and Luteciel SARL*; Case C-238/08 *Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others* (23 March 2010).

[452] Case 70-10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4 [53].

[453] Case 360-10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* [2012] ECR I-0000 [51].

[454] Case 484/14 *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH* [2016] [87].

see for instance *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017). Equally, the notice and staydown approach has also been heavily criticised by the UN Special Rapporteur on Freedom of Expression for its total disregard of human rights (see Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda at pg 2).

7. On the one hand, academics such as, Mendis[455] and Lucas-Schloetter[456] argue that this is an area that needs consideration and the online platforms should be placed with a higher burden to monitor users' activities such as, relying on notice and staydown measures. They claim that there has to be a greater burden on online platforms to moderate harmful content and the legal liability for online platforms should differ according to the harm suffered. The more prominent online platforms have software to detect material that is deemed harmful and therefore will not be posted. Such measures should be adopted by all online platforms thereby making a distinction between avoiding harm on the one hand and bearing the liability in accordance with the harm caused due to lack of swift action on the part of the online platform.

8. Conversely, a growing body of legal scholarship has warned of the risks and challenges associated with content recognition and filtering systems. They argue that under Article 14 and 15 of the E-Commerce Directive, EU law and CJEU case law, online platforms should not be required to proactively monitor, filter and block content uploaded by their users.[457] Equally, Member States have argued that notice and staydown measures could be incompatible with both the EU Charter and CJEU case-law. For example, Belgium, Czech Republic, Finland, Hungary, Ireland, the Netherlands[458] and Germany[459] have claimed that in *Sabam v Netlog* and *Sabam v Scarlet* the CJEU declined to impose a duty on

[455] D Mendis and D Secchi, *A Legal and Empirical Study of 3D Printing Online Platforms and an Analysis of User Behaviour* (London: UK Intellectual Property Office; 2015).

[456] Lucas-Schoetter, Agnès. 2017. "Transfer of value provisions of the Draft Copyright Directive (recitals 38, 39, article 13)." http://www.authorsocieties.eu/uploads/Lucas-Schloetter%20Analysis%20Copyright%20Directive%20-%20EN.pdf

[457] See for instance Senftleben et al. 2017. "The Recommendation on measures to safeguard fundamental rights and the open internet in the framework of the EU Copyright Reform." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3054967; Stalla-Bourdillon et al. 2016. "A brief exegesis of the proposed Copyright Directive." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2875296; Angelopoulos. 2017. "On online platforms and the Commission's new Proposal for a Directive on Copyright in the Digital Single Market." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2947800; Angelopoulos and Smet. 2016. 'Notice-and-Fair-Balance: How to reach a compromise between fundamental rights in European intermediary liability' https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2944917; Giancarlo Frosio. 2017. "Reforming intermediary liability in the platform economy: a European Digital Single Market Strategy." *Northwestern University Law Review* https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2912272; Bridy and Keller. 2017. "US Copyright Office Section 512 Study [Docket no 2015-7] Comments of Annermarie Bridy and Daphne Keller." https://www-cdn.law.stanford.edu/wp-content/uploads/2017/08/SSRN-id2920871.pdf; Jennifer M Urban, Joe Karaganis, and Brianna L Schofield. 2016. "Notice and takedown in everyday practice." *BerkeleyLaw University of California*: 1-147. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628; Evan Engstrom, and Nick Feamster. 2017. "The limits of filtering: a look at the functionality and shortcomings of content detection tools." Engine: 1-32. http://www.engine.is/the-limits-of-filtering/.

[458] Council of EU. 2017. "Document 12127/17, Interinstitutional File 2016/0280 (COD), Proposal for a Directive on the European Parliament and of the Council on Copyright in the Digital Single Market – Questions by the Belgian, Czech, Finnish, Hungarian and Dutch Delegations to the Council Legal Service Regarding Article 13 and Recital 38."

[459] Council of EU. 2017. "Document 12291/17, Interinstitutional File 2016/0280 (COD), Proposal for a Directive on the European Parliament and of the Council on Copyright in the Digital Single Market – Questions by the German Delegation to the Council Legal Service Regarding Article 13."

service providers to automatically monitor the contents disseminated by their users on the basis of Articles 8, 11 and 16 of the Charter. Additionally, current research has found that notice and staydown measures could also violate the rights of online platforms and users under Articles 6, 8 and 10 of the European Convention on Human Rights.[460]

3. How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

1. When signing up to the use of online platforms, users inadvertently, sign up to various terms and conditions – which for most users can be confusing and complex and may not always be clear to the average user. Yet, when an issue arises, an online platform can point to the terms and conditions, with ease.

2. In 2015, a commissioned report for the UK Intellectual Property Office exploring online platforms and user behaviour in the context of platforms dedicated to the sharing of 3D files, established that 65% of users did not license their work, leaving their creations vulnerable and open to infringement whilst losing the ability to claim authorship (Mendis and Secchi, 2015).[461] When an issue arose in relation to the copyright content, the online platforms considered in this Study were able to point to their terms and conditions and user agreements, thereby avoiding liability for the content that they host. Therefore, *transparency* could be improved.

3. This could be achieved by online platforms providing more awareness and understanding of their terms and conditions, and offer it in a manner that is more user friendly. For example, the nuances relating to each licence, could be explained in clear and simple language, rather than simply 'encouraging' the user to adopt a particular type of licence.

4. In terms of efficiency, online platforms have a legal liability to take swift measures to stop an infringing activity, rather than resorting to court procedures. However, there is no quantified requirement from statutes or jurisprudence regarding how *quickly* the information should be removed upon obtaining such knowledge. In practice, internet intermediaries tend to swiftly respond and remove the infringing information. For example, in the case of counterfeited goods, intermediaries have been known to remove the material within three days or even shorter.

5. With regard to appeal processes, users should be provided with complaint mechanisms in the case of disputes and any technical solution should also be compatible with the rights of online platforms and users to a fair trial under Article 6 of the European Convention on Human Rights. Specifically, pursuant to the Strasbourg Court equality of arms principle, online platforms should be

[460] Romero-Moreno. 2018. ''Notice and staydown' and social media: Amending Article 13 of the Proposed Directive on Copyright.' *International Review of Law, Computers & Technology* (in press) - email f.romero-moreno@herts.ac.uk for a free copy.

[461] D Mendis and D Secchi, *A Legal and Empirical Study of 3D Printing Online Platforms and an Analysis of User Behaviour* (London: UK Intellectual Property Office; 2015)

required to quickly notify users when material that they generated, uploaded or host might be subject to a technical measure.[462] Moreover, following this principle, users should also be given an opportunity to respond to any technical measure.[463] For instance, as in the US (DMCA 1998) and some EU countries, users should be notified of takedowns requests and be given the opportunity to send counter-notices to the service provider requesting that their uploaded content be reinstated, thereby relying on 'put-back' processes. The courts or the data protection supervisory authorities such as, the Information Commissioner's Office could be responsible for overseeing this - in this context see eg Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsenk* [2016] All ER (D) 107 (Dec) and *Secretary of State for the Home Department v Tom Watson* [2016] All ER (D) 107 (Dec) [123]; and *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [122].

4. What role should users play in establishing and maintaining online community standards for content and behaviour?

1. It must be recognised that online communities whilst sharing some key characteristics with offline communities are fundamentally different in their composition,[464] and in what is deemed as acceptable behaviour. It would therefore be a mistake to try and impose one set of standards on all online communities but also to expect that they will adopt the same standards in respect of behaviour that we see offline.

2. Where considerations of user involvement in establishing and setting standards for content and behaviour are made, this is in itself likely to mean that there are different standards for each online platform. Users feel part of communities where they engage online – in some online communities, experiments concerning governance have involved users setting standards.[465]

3. Involving users in establishing and maintaining community standards should offer the opportunity to enhance the standards adopted. Ultimately, there are already standards for content and behaviour set out by social media platforms and other online communities.[466] The problem here is that users often fail to read the documents outlining these standards[467] but beyond that, where there is a contravention, then the enforcement of these standards is often problematic – in that the standards do not address the objectionable behaviour,

[462] Refer to the Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21287&LangID=E at pg 4; see also *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [133].

[463] See Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21287&LangID=E at pg 4; see also the CJEU C-314/12 UPC *Telekabel Wien GmbH v Constantin Film Verleih GmbH and anor* [2014] All ER (D) 302 (Mar) [57].

[464] See for example, K Barker & C Baghdady, 'Building online hybrid identities' in N Lemay-Herbert and R Freedman (eds) Hybridity: Law, Culture and Development (Routledge, 2017).

[465] K Barker (2016): Virtual spaces and virtual layers - governing the ungovernable?, Information & Communications Technology Law, 25:1, 62 70; J Dibbell, 'A Rape in Cyberspace' 23 December 1993, http://www.juliandibbell.com/texts/bungle_vv.html.

[466] See for example: Twitter Rules & Policies https://help.twitter.com/en/rules-and-policies#twitter-rules.

[467] A point widely commented on e.g. D Berreby, 'Click to agree with what? No one reads terms of service, studies confirm' The Guardian, 3 March 2017 https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print.

or the platform seeks not to enforce measures against the user in contravention.[468]

4. The Internet Safety Strategy document sets out the Government's intent to improve safety online[469] – establishing and maintaining online community standards for content and behaviour should fall within that remit. However, simply imposing a code of conduct on the online communities will not satisfy this desire. The EU IT Companies Code of Conduct[470] is one aspect of establishing standards but it is only one aspect and does not involve users.

5. Given that users of these online communities are the ones who will be either upholding or breaching these standards of behaviour, it is important that their opinions be canvassed. That said, it is important to note that simply because something is offensive, it is not necessarily something which is illegal and this is a fine line which needs to be recognised in establishing standards, and which is consistent with the established principles of freedom of expression.

5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

1. Any measures adopted – such as those including reporting and reviewing – must maintain a proportionate balance between posts which are removed, and those which are upheld on the basis of being questionable but not posing a problem.

2. Simply adopting measures does not mean that the rights will be protected.

3. Freedom of Expression (FoE), and Freedom of Information (FoI) are not the only rights which ought to be protected online. All rights ought to be protected but nevertheless the FoI provisions are likely to be enhanced following the introduction of the GDPR (see below). The FoE rights need greater protections given that filtering, moderating, and muting[471] are arguably all threats to FoE online.

4. Platforms need to balance FoE rights with maintaining standards for content and behaviour, but also whilst maintaining participation rights[472]. The freedom of participation is also essential for the Internet and for users of online communities/platforms and therefore this must also be considered alongside FoE and FoI.

[468] See for example, Twitter's criticism for failing to deal with hateful tweets: J Grierson, 'Twitter fails to deal with far-right abuse, anti-hate crime group tells MPs' The Guardian, 13 December 2016: https://www.theguardian.com/technology/2016/dec/13/twitter-fails-deal-farright-abuse-tell-mama-extremism-commons.

[469] HM Government, 'Internet Safety Strategy – Green Paper' October 2017.

[470] European Commission, 'European Commission and IT Companies announce Code of Conduct on illegal online hate speech' (31 May 2016) http://europa.eu/rapid/press-release_IP-16-1937_en.htm.

[471] Which are all mechanisms used by social media platforms to tackle posts and behaviour in breach of their respective terms and conditions.

[472] See for example, Internet Rights and Principles Coalition, 'The Charter of Human Rights and Principles for the Internet' (5th edn) 2018: http://internetrightsandprinciples.org/site/wp-content/uploads/2018/01/IRPC_english_5thedition.pdf.

5. It is essential that the UK does not follow the example of Germany and introduce measures replicating that of NetzDG[473] which is a direct challenge to FoE online. Such measures are not conducive to maintaining online safety whilst protecting rights. Reporting, flagging and reviewing posts and online content is the predominant method by which unacceptable content is addressed – notably through takedown steps. Whilst this does not ensure the FoE rights are upheld, it is a retrospective – and therefore reactive – approach. The current approach in terms of 'illegal content'[474] is not an ideal solution but is one which has shown results in respective of extremist content[475]. This approach could be rolled-out to incorporate an assessment of the balance between FoE/FoI and online safety.

(i) 6. Some of these measures are outside of the control of social media platforms e.g. No Hate Speech Movement[476] – there is also a place for these campaigns.

6. What information should online platforms provide to users about the use of their personal data?

1. First and foremost, platforms need to provide information as required by the General Data Protection Regulation 2016 (GDPR) and the Data Protection Bill 2017 (DP Bill). Platforms need to abide by the principles of transparency and accountability, enshrined in GDPR and representing crucial changes in the revised data protection regime[477].

2. Practically, this means that they need to explain the use of personal data in a concise, transparent, intelligible and easily accessible manner, using clear and plain language[478]. This must be in it must be in writing "or by other means, including where appropriate, by electronic means", orally if requested by a data subject as well as free of charge[479].

3. Information that need to be provided to data subject under the law include: the identity and contact details of the platform; contact details for the data protection officer; the purposes and legal basis for the processing; where legitimate interests (Article 6.1(f) GDPR) is the legal basis for the processing, the legitimate interests pursued by the data controller or a third party; categories of personal data concerned; recipients of the personal data; details of transfers to third countries and the details of the relevant safeguards; the

[473] Germany's Network Enforcement Act (NetzDG) 2017. See: Beschlussempfehlung und Bericht [Resolution and Report], Deutscher Bundestag: Drucksache [BT] 18/13013, http://dipbt.bundestag.de/doc/btd/18/130/1813013.pdf; BBC News, 'Germany starts enforcing hate speech law' 1 January 2018: http://www.bbc.co.uk/news/technology-42510868

[474] EU Commission, 'Commission Recommendation on Measures to Effectively Tackle Illegal Content Online' 1 March 2018.

[475] EU Commission, 'Countering Illegal Hate Speech Online' (19 January 2018) http://europa.eu/rapid/press-release_MEMO-18-262_en.htm.

[476] No Hate Speech Movement: https://www.nohatespeechmovement.org/hate-speech-watch/focus

[477] Article 5 GDPR, related to articles 1, 11 and 15 TFEU, see also Article 29 WP Guidelines on transparency under Regulation 2016/679, WP 260, p. 5, at https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[478] Article 29 WP interprets intelligible as 'it should be understood by an average member of the intended audience' Article 29 WP Guidelines, p.7.

[479] See Articles 12-15 and 22 GDPR.

storage period (or criteria used to determine that period), the rights of users to: access; rectification; erasure; restriction on processing; objection to processing and portability (articles 15-22 GDPR); where processing is based on consent, the right to withdraw consent at any time; he right to lodge a complaint with the ICO; whether there is a statutory or contractual requirement to provide the information or whether it is necessary to enter into a contract or whether there is an obligation to provide the information and the possible consequences of failure; the source from which the personal data originate; the existence of automated decision-making including profiling and, if applicable, meaningful information about the logic used and the significance and envisaged consequences of such processing for the user[480].

4. Practically, this could be done using innovative visualisation techniques, such as layered privacy statements/notices (link to the various categories of information which must be provided to the data subject as suggested above in order to avoid information fatigue),[481] 'push' and 'pull' notices[482] and privacy icons[483].

5. It is crucial that the UK follows standards for digital and online advertising as set by the ongoing EU reforms as well as in accordance with GDPR and consumer protection laws. It is important that platforms acknowledge relationships and overlap between these areas of law and how they affect user rights to privacy and freedom of speech. This necessity is often disregarded in practice and even in the academic discourse.

6. However, as recent scandals show (Cambridge Analytica in particular), providing all the information required by the law is far from sufficient. Platforms need to be clear as to what business model they use and what does this mean for user and their fundamental rights more generally, not limited to the right to private and family life. There should be clear prohibition of manipulative practice, akin to Cambridge Analytica, which may influence democratic processes, user autonomy and the ability to make an informed decision about their participation in social and economic processes.

7. It is also essential that intermediaries provide information regarding the use of the deceased's data and their related policies. Many platforms lack these

[480] Articles 13-14 GDPR and Article 29WP Guidelines on transparency, pp. 30 – 35.

[481] Article 29WP opinion p. 17; see also Office of the Australian Information Commissioner. Consultation draft: Guide to big data and the Australian Privacy Principles, 05/2016 says: "Privacy notices have to communicate information handling practices clearly and simply, but also comprehensively and with enough specificity to be meaningful. The very technology that leads to greater collection of personal information also presents the opportunity for more dynamic, multilayered and user centric privacy notices." https://www.oaic.gov.au/engage-with-us/consultations/guide-to-bigdata-and-the-australian-privacy-principles/consultation-draft-guide-to-big-data-and-the-australian-privacyprinciples; Information Commissioner's Office – Big data, artificial intelligence, machine learning and data protection version 2.0, 03/2017. Pp 87-88, March 2017. https://ico.org.uk/media/fororganisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

[482] Push notices involve the provision of "just-in-time" transparency information notices while "pull" notices facilitate access to information by methods such as permission management, transparency dashboards and "learn more" tutorials. These allow for a more user-centric transparency experience for the data subject. Article 29WP Guidelines on transparency, p. 17.

[483] Article 12 GDPR Recital 166; Article 29WP Guidelines on transparency notes the need for more research around icons, p. 22 Opinion; ICO, Big data, artificial intelligence, machine learning and data protection version 2.0, pp 62-65.

policies, and a lot of the existing policies are not compliant with the UK data protection, copyright and succession laws.[484] Whole identities are created and stored online, so users should be able to decide what happens to data on these platforms after they die, otherwise we risk seeing more conflicts between platforms, friends and the deceased's family, who wish to access different accounts. All this of course notwithstanding any public interests, such as historical and archival purposes for example. This information needs to be clearly presented to users in an intelligible and simple manner, using some of the techniques described above.

8. Looking beyond data protection laws, intermediaries also need to explain how they use user data in managing requests related to copyright infringement, defamation and the law enforcement, as noted in answers to the previous questions. Some reference to the UK law should be in place here, presented in an easily understandable language, as suggested above.

7. In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

1. Individuals may find it challenging to understand the complex techniques involved in profiling and automated decision-making processes, including the use of AI, machine learning and algorithms. It has been evidenced that profiling may be unfair and generate discrimination, (by denying individuals access to employment opportunities, credit or insurance, or targeting them with excessively risky or costly financial products).[485] Generally, platforms need to explain their business models and the way they use personal data of their users, as well as what effect this processing can have/has on individuals. If their business model is not based on using personal data for advertising, it should still be set out in clear terms.

2. To improve transparency and address shortcoming of GDPR with regards to the use of algorithms,[486] transparency should not be limited to GDPR-related obligations only and mostly to public bodies.[487] Also, platforms should not only be requiring to provide information only about the use of purely personal data but also aggregate data they claim to be anonymous (and there is much

[484] See e.g. Edina Harbinja, Digital Inheritance in the United Kingdom, 21 Nov 2017, The Journal of European Consumer and Market Law (EuCML); Harbinja, Post-mortem Privacy 2.0: Theory, law and technology, (2017) International Review of Law, Computers & Technology. 31 (1) p. 26-42.

[485] Article 29 WP, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, p. 10.

[486] Lilian Edwards and Michael Veale, Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For, 16 Duke Law & Technology Review 18 (2017); Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling, Computer Law & Security Review 34(2) 2018, 398–404, doi:10.1016/j.clsr.2017.12.002; Sandra Wachter, Brent Mittelstadt and Luciano Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, International Data Privacy Law, 2017.

[487] Articles 13 and 14 require the controller to inform the data subject about the existence of automated decision-making, including profiling, described in Article 22(1) and (4). addressed in Articles 13 and 14 – specifically meaningful information about the logic involved, as well as the significance and envisaged consequences for the data subject), and safeguards, such as the right to obtain human intervention and the right to challenge the decision (addressed in Article 22(3)) p. 25.

evidence that any data can be linked back and reidentified, if adequate techniques have not been used to anonymise the data fully).[488]

3. Providing a complex mathematical explanation about how algorithms or machine-learning work is not helpful for an average user, as they would not be able to grasp the full meaning of these. Instead, platforms should consider using controller should consider using innovative solutions to provide information to their users, such as, for instance visualisation tools, simple design and adequate notices as discussed above.[489]

4. As suggested by the Article 29 Working Party, the information provided to users about profiling and automated decision-making should include for example: the categories of data that have been or will be used; why these categories are considered pertinent; how any profile used in the automated decision-making process is built; why this profile is relevant to the automated decision-making process; and how it is used for a decision concerning the user.[490]

5. In addition, it is not sufficient to explain how the decision was made but also whether there is an opportunity for a revise by a human and in its absence, why not. A user should be able to access the results, correct and challenge the decision made by an algorithm (going beyond article 22 GDPR, which focuses on automated processing ***with significant or legal effect*** on data subjects, not authorised by consent or contract, but by member state law). As suggested by Veale, Binns and Edwards, safeguards should include a meaningful right to explanation; a requirement for meaningful human involvement in certain decisions; and a right to complain and seek effective judicial redress as a result of the consequences of an automated decision.[491] We support this stance.

8. What is the impact of the dominance of a small number of online platforms in certain online markets?

1. Frequently labelled as the 'Big Four' of the tech moguls, it is arguable that, in the future, Google, Amazon, Facebook and Apple (the GAFAs) will continue to have powerful influence on the way humans work and live. It is likely that the GAFAs will keep acquiring clever startups, which serve as a business alternative to the usual service in the internet era. Since 2001, Google has acquired more than two hundred startups such as, DeepMind. In 2016, Google CEO Sundar Pichai stressed that developments in AI, data management, infrastructure and analytics would be carried out in the cloud. Similarly, in 2017, among its nine

[488] See President's Council of Advisors on Science and Technology. Big data and privacy. A technological perspective. White House, May 2014 http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf and also El Emam, Khaled. Is it safe to anonymise data? BMJ, February 2015. http://blogs.bmj.com/bmj/2015/02/06/khaled-el-emam-is-it-safe-to-anonymize-data/

[489] See also ICO, Big data, artificial intelligence, machine learning and data protection version 2.0, pp 87 - 88

[490] Article 29 WP, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, p. 31.

[491] See Public Bill Committee, Written Evidence: Michael Veale, UCL, Dr Reuben Binns, University of Oxford, Professor Lilian Edwards, University of Strathclyde (DPB03), 14 March 2018, at https://services.parliament.uk/bills/2017-19/dataprotection/documents.html

acquisitions, Amazon purchased Graphiq. This was remarkable as an AI-based tech business, which created charts relying upon searchable data sets. By the same token, according to Facebook CEO Mark Zuckerberg, AI can and should be employed to better humanity. In addition to Facebook's acquisition of Instagram, the social network's purchase of companies such as the virtual reality service Oculus clearly feed into this plan. Additionally, in 2017, of the seven purchases and teams-ups by Apple, particularly significant were the acquisitions of Lattice Data that concentrates on processing unstructured data, and Initial, a messaging virtual assistant. The latter employs natural language processing (NLP). Equally, Apple's services SensoMotoric and Regaind specialize in computer vision.[492]

2. Despite the fact that trust in these tech moguls is being questioned due to concerns regarding fake news, misuse of personal data and tax avoidance, arguably a potential next step would be for the GAFAs to leverage a mixture of customer, product and global economic data to provide economic advice and targeted product information.[493] As Fintank has noted, '*using mapping data from Google, iTunes information from Apple, social media content from Facebook and customer choices from Amazon, this vast customer insight could lead to highly personalised financial advice and solutions.'*[494]

3. However, a case can be made that it is not the GAFAS the tech moguls that one should be concerned about. China's internet giants Baidu, Alibaba and Tencent (the BATs) are now taking the lead, interacting with customers beyond China's boundaries and posing a risk to the global financial marketplace.[495] In fact, the BATs seem to be much more active and dynamic than the GAFAs.[496] Yet, if the BATs were to expand beyond Asian borders, these internet giants will need to do so under the same burdensome legal regimes, which the GAFAs work. Perhaps, whilst the GAFAs will influence the concept of global banking, financial institutions will have to move to the places in which clients spend their time that is, the GAFAs' apps. App usage largely focuses on social networks, Google and utilitarian apps like messaging and maps. Thus, in the future, banks will likely find themselves wholly engaged in the apps their clients use the most. For instance, services such as Google Maps, Facebook's Messenger and WhatsApp as well as Amazon's Alexa virtual assistant.[497]

[492] Nina Bryant, 'Blink of an AI' (ICAEW Communities, April 2018) < https://ion.icaew.com/itcounts/b/weblog/posts/blink-of-an-ai > accessed 29 April 2018.

[493] Simon Cadbury, 'Will a GAFA be your next bank' (Intelligent Environments) < https://www.intelligentenvironments.com/will-gafa-next-bank/ > accessed 29 April 2018.

[494] *Ibid*., accessed 29 April 2018.

[495] Alibaba's Ant Financial launched MyBank, a digital bank aimed at those who have restricted access to current banking systems and corporations seeking financing, in June 2015; Tencent launched WeBank, that is closely integrated with the notable Chinese instant messaging app WeChat, in January 2015; Baidu – 'the Google of China' – and partner CITIC Bank were given approval to launch a new joint banking operation last August - see *Ibid*., accessed 29 April 2018.

[496] Ant Financial is on the acquisition and expansion trail, investing directly in online wallets such as South Korea's Kakao Pay and India's Paytm, and attempting to purchase MoneyGram for $1.2bn; Tencent is leveraging WeChat to enlarge its geographic coverage; Baidu and its partners' ambitions exceed payments, with Baixin Bank leveraging Baidu's AI - see Ibid., accessed 29 April 2018.

[497] WeChat: China Construction Bank, Bank of China, and China Merchants Bank are just three of many banks, which have used chatbots on WeChat; Alexa: Capital One clients can manage their accounts via Amazon's voice-enabled chatbot; Facebook Messenger: Citibank's natural-language chatbot called Citi Bot permits clients to ask questions regarding their accounts, rewards and transactions - see Ibid., accessed 29 April 2018.

4. We believe that these issues of dominance cannot be addressed by competition law only, as this area of law is reactive and *post factum*, and it does not take into account vendors lock-in, network externalities and economies of scale and scope. Regulation here should rather be *ex ante,* focusing on the measures that would improve interoperability and the mobility of users.

9. What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

1. The UK government plans to exclude the Charter of Fundamental Rights of the European Union 2000 from 'EU retained law' after Brexit.[498] Instead, underlying principles and rights will continue and will be substitute reference points in pre-Brexit case-law making reference to the EU Charter.[499]

2. However, when it comes to the regulation of the internet, this raises a number of issues. For example:

- Will the UK depart from aspects of the E-commerce Directive 2000/31/EC once it is transferred into domestic law? A specific problem would be that Article 15 of Directive 2000/31/EC[500] has not been transposed into the UK E-commerce Regulations. Therefore, it will not be retained under the Withdrawal Bill. We believe that this needs to be addressed in law.

- What will the position of UK internet intermediaries be in terms of their operation in EU27? Simple incorporation of EU law as domestic law will not work as from an EU law point of view, the UK may (without a 'deal') be a third country and so an intermediary is not established in a member state.[501]

3. More generally, there will be great pressure for deregulation after Brexit. A key issue is the e-Privacy Regulation Proposal, currently discussed in the EU and the fact that the UK will exit before it comes into effect.[502]

4. Perhaps unsurprisingly, in 2017, the Lords Select Committee on the EU stressed that it was 'struck by the lack of detail' on what effect will the UK

[498] Commons Library Briefing, 'Brexit and data protection' (10 October 2017) https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7838#fullreport at page 4.

[499] *Ibid*.

[500] Article 15 of the E-Commerce Directive has not been transposed in the UK E-Commerce Regulations. Thus, this means that it will not be retained under the Withdrawal Bill. However, it is important to stress that the Withdrawal Bill must 'take into account' the ECtHR and CJEU case-law. Accordingly, if Article 15 E-Commerce Directive is scrapped this would be inconsistent with the UK obligation to take into consideration the rulings of both courts. In this context see for example Case 70-10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4; Case 360-10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* [2012] ECR I-0000; Case 484/14 *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH* [2016]; and *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017); for an in-depth analysis of this issue see Romero-Moreno. 2018. ''Notice and staydown' and social media: Amending Article 13 of the Proposed Directive on Copyright.' *International Review of Law, Computers & Technology* (in press) - email f.romero-moreno@herts.ac.uk for a free copy.

[501] With special thanks to Professor Daithi Mac Sithigh.

[502] With special thanks to Dr Edina Harbinja.

leaving the EU have on internet law.[503] In fact, the Committee warned that there was no prospect of a 'clean break' from the EU.[504] It is noteworthy that, as of 23rd April 2018, peers in the House of Lords voted by a majority of 71 opted to retain most of the Charter of Fundamental Rights of the European Union 2000 in UK domestic legislation after Brexit.[505]

5. Moreover, it should also be observed that the legally binding character of the EU Charter in 2009 did not deprive the European Convention on Human Rights 1950 of its role as a source of fundamental rights protection in the EU. The Treaty of Lisbon 2007 has paved the way to EU accession to the ECHR. However, in 2015 the Court of Justice of the European Union found that the negotiated agreement neither provided the CJEU's exclusive jurisdiction, nor sufficient protection concerning the EU's specific legal arrangements. Thus, although both the European Parliament and the European Commission stress the need for EU accession, as of today, a new draft accession agreement is still waiting.[506]

6. Furthermore, it is worth pointing out that the CJEU interprets the instruments, directives and regulations in line with the EU Charter. This means that equivalence, adequacy or compatibility of UK law will be assessed by the European Commission in view of the interpretation of UK law by the CJEU after Brexit. Accordingly, when such assessment is carried out, the CJEU case-law must be 'taken into account'.[507]

7. Importantly, in assessing the relationship between the ECHR and the EU Charter, in the CJEU decision in *Tele2/Watson*, the Advocate General Saugmandsgaard-Øe advised that, according to Article 6(3) Treaty on the European Union 2007, human rights as enshrined in the ECHR, constituted general principles of EU law. However, the AG acknowledged that since the EU had not acceded to the Convention, the latter could not be considered a legal instrument, which had been formally incorporated into the Union's law.[508] The AG elaborated that EU law did not preclude the Charter from offering more extensive protection than that available in the Convention.[509] Thus, AG Saugmandsgaard-Øe concluded that when it comes to assessing human right issues, it would not be legally correct to impose a different test on Member States such as the UK, depending on whether the ECHR or the EU Charter was

[503] House of Lords European Union Commitee, 'Brexit: the EU data protection package' HL Paper 2017-19, 18 July 2017 https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/7/7.pdf at pg 3.

[504] *Ibid*., at pg 51.

[505] Andrew Sparrow, 'May suffers three defeats in Lords over Brexit - as it happened' (The Guardian) < https://www.theguardian.com/politics/blog/live/2018/apr/23/brexit-no-10-rejects-claims-customs-union-vote-to-be-made-a-confidence-issue-politics-live?page=with:block-5ade16fae4b0d0cf980b8ee4 > accessed 29 April 2018.

[506] European Parliament Think Tank, 'EU accession to the European Convention on Human Rights (ECHR)' < http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI%282017%29607298 > accessed 29 April 2018.

[507] Oral evidence to the Select Committee on the European Union Home Affairs Sub-Committee, 1 March 2017, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-home-affairs-subcommittee/eu-data-protection-package/oral/48742.pdf at pg 8.

[508] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsenk* [2016] All ER (D) 107 (Dec) and *Secretary of State for the Home Department v Tom Watson* [2016] All ER (D) 107 (Dec) [AG 76].

[509] *Ibid*., [AG 80]

being examined.[510] Indeed, in addition to *Tele2/Watson*, the CJEU ruling in *Digital Rights Ireland*[511] also reflects how the case-law of the Strasbourg and Luxembourg Court is increasingly becoming carefully 'aligned'.[512]

8. It should be noted that the European Court of Human Rights and CJEU alignment of case law appears to be also increasingly acknowledged by the UK courts – see for instance the internet law decisions in *Cartier International AG and Others v British Sky Broadcasting Limited and Others* [2014] EWHC 3354, *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors* [2016] EWCA Civ 658 (06 July 2016), *The Football Association Premier League Ltd v British Telecommunications Plc & Ors* [2017] EWHC 480 (Ch) (13 March 2017) and *SSHD v Watson & Others* [2018] EWCA Civ 70. Thus, in view of the above, it is perhaps arguable that the UK government would be wise to abandon its plans to scrap the EU Charter after Brexit.

Response Prepared by:
Dr. Kim Barker, (Lecturer in Law, University of Stirling);
Dr. Edina Harbinja (Senior Lecturer in Law, University of Hertfordshire);
Prof. Dinusha Mendis (Professor of Intellectual Property & Innovation Law, Bournemouth University); and
Dr. Felipe Romero-Moreno (Lecturer in Law, University of Hertfordshire)

On behalf of the British and Irish Law, Education and Technology Association (BILETA).

Response Endorsed by:
Professor Abbe E. L. Brown, Law School, University of Aberdeen
Dr Maureen O Mapp, Lecturer in Law, Birmingham Law School, University of Birmingham
Dr Gavin Sutter, Senior Lecturer in Media Law, CCLS, School of Law, Queen Mary University of London
Bukola Faturoti, Senior Lecturer, The Law School, Robert Gordon University.

11 May 2018

[510] *Ibid.*, [AG 142]

[511] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others* [2014] WLR (D) 164.

[512] Legal opinion by the Legal Service of the European Parliament (confidential legal opinion 22 December 2014) 9 – with special thanks to Dr Sonia Morano-Foadi; for an in-depth analysis of the ECtHR and CJEU alignment of internet case-law see Romero-Moreno. 2018. ''Notice and staydown' and social media: Amending Article 13 of the Proposed Directive on Copyright.' *International Review of Law, Computers & Technology* (in press) - email f.romero-moreno@herts.ac.uk for a free copy.

Mark Bunting and Dr Damian Tambini – oral evidence (QQ 12-20)

Tuesday 1 May 2018

Watch the meeting

Members present: Lord Gilbert of Panteg (Chairman); Baroness Bertin; Baroness Bonham-Carter of Yarnbury; The Lord Bishop of Chelmsford; Viscount Colville of Culross; Lord Goodlad; Lord Gordon of Strathblane; Baroness Kidron; Baroness McIntosh of Hudnall.

Evidence Session No. 2 Heard in Public Questions 12 - 20

Examination of witnesses

Dr Damian Tambini, Associate Professor, Department of Media and Communications, London School of Economics; Mark Bunting, Partner, Communications Chambers.

Q12 **The Chairman:** I welcome the witnesses who are giving evidence to our inquiry on internet regulation.

Our Committee has published a number of recent reports containing recommendations on regulation of the internet. The subject generates much public debate and policy-making. We are now looking at whether there needs to be a comprehensive and strategic regulatory framework, whereby we balance the need for regulation with freedom of expression. We are going to review how the internet has come to be regulated, both in the UK and internationally; assess calls for further regulation; and make recommendations about how the internet should be regulated in the future.

I advise the witnesses that the session is being recorded and transmitted and a transcript will be taken. Our witnesses are policy experts, Dr Damian Tambini and Mark Bunting. In introducing yourselves, can you tell us a bit about who you are and your background? So that we can understand where you are coming from on these issues, could you tell us whether in your view there is a need for a new regulatory framework for the internet and, if so, what form you favour? Is it one of self-regulation, more directed co-regulation or direct regulation?

Dr Damian Tambini: Good afternoon, and thank you very much for inviting me. I am research director of the department of media and communications at the London School of Economics.

I agree that there is a need for a comprehensive new set of principles and institutions to deal with the kind of issues that the Committee has identified. If we step back a bit, to understand what has been happening in this space, we see that the Government’s internet safety strategy is only part of the picture. Across the piece, we have been delegating censorship functions or regulatory functions to the platforms to deal with a variety of social problems, from child safety to fake news and intellectual property infringement. Partly as a result of that, those platforms have become immensely powerful in their decision-making and curation of themselves, and are having an effect on people's enjoyment of their fundamental rights.

The Committee is absolutely right to identify the problem of balancing freedom of expression and regulation in that complex co-regulatory framework, but we need to examine an institutional solution that would work better than the current fits and starts, where there are all sorts of problems of material not being taken down or being taken down too quickly, overblocking and a situation in which rights are not really respected.

Mark Bunting: I am a partner at Communications Chambers, an advisory firm specialising in media and telecoms policy. I worked at Ofcom between 2004 and 2008, so I have some hands-on exposure to the joys of content regulation and broadcasting policy. I then spent eight years at the BBC. Last year, as a visiting fellow at the Oxford Internet Institute, I worked on a project on the applicability and options for content regulation online, which is obviously one of the areas you are most focused on. By way of a brief disclosure, I should say that, as an adviser, my clients include technology companies, DCMS and broadcasters. I am currently working on a project funded by Sky looking at options for online content regulation.

To give you a fairly brief answer to the question, I hope, it is important to be specific about where we think the problems and gaps may be in internet regulation. The current issues generating so much attention fall broadly into three buckets: data and privacy, particularly with the Cambridge Analytica and Facebook controversies of recent weeks; online content and platforms' role in regulating content; and competition, which I know you want to talk more about later.

To my mind, the most obvious gap is in content regulation, which is why I have been working in that area for the past 18 months. To be more specific about the gap, it is not so much in the rules about what kinds of content are legal or not; it is more in the creation of regulatory capacity to engage with platforms' role in managing access to that content. As Damian said, we need to find ways of institutionalising a different kind of relationship with the intermediaries that govern access to content to ensure that the principles of good governance are met.

Q13 **Baroness Kidron:** That is very interesting. Can I ask you the traditional question? Are they platforms or are they publishers? In answering that, can you also let us know whether you think we are due a new definition, and whether part of the problem with asking the question is that we have not asked it in a comprehensive way? Perhaps you would deal with that first and then I will come to another point.

Dr Damian Tambini: Legally, they are platforms; they have a shield from liability until they are notified that they are hosting something potentially illegal. I think there is emerging consensus that we have reached a situation where the law needs to catch up in some way, and there needs to be an intermediate category between publishers and mere conduits. That is easier to say than it is to do. Legally, even in the UK, once you click on that narrow question and open it up, how the law treats you as a publisher depends on the different legal area you are speaking about, so intellectual property would be very different from defamation and so forth.

The idea that there should be a complete shield from liability goes back to the 1990s when there was a new thing called the internet and we wanted to foster innovation and economic growth by giving it a shield from liability. We have moved on to a situation where there is a small number of very powerful monopoly players, and oligopolies in some markets, and what has been called an indirect subsidy of the liability shield needs to be opened up and reviewed.

Mark Bunting: As a matter of law, things have to be capable of clear definition and we have to know which categories organisations sit in. As a matter of policy, I do not think the definitional game is a very helpful one to play, with no offence intended to the question.

Baroness Kidron: That is fine. That is what we are here to discover.

Mark Bunting: The starting point for policy is: what is the activity that is systematically likely to lead to consumer or citizen harm, or to missed opportunities for citizen and consumer benefits, which is the other side of the coin? The activity that is not well addressed by existing law or regulation is the role that intermediaries now play not just as a conduit for content but in actively curating, as the buzzword goes, that content, by which I mean that they select which content is presented to users; they rank that content; they recommend content; and they moderate content. You cannot do that in a purely neutral way; you have to do it by setting the values that you want to optimise in the searching of content.

In markets where exposure to content is so important to fundamental rights, as Damian says, and to all sorts of public goods, including the effective functioning of democracy, the values that intermediaries bring to bear on the task of curating content seem to me a legitimate issue of public policy. Interventions that enable us to get better at seeing how they do that, and what the effects are of that curatorial function, seem to be the things we ought to be trying to identify.

Baroness Kidron: A question that really interests the Committee is the design of services. You said that the problems lie in the three buckets of data privacy, content and competition, but there are worries about the actual design of services—for example, if you read last week’s testimony, design to addict. What role does that have in understanding what one is dealing with in terms of definition or non-definition—however you wish to answer it—and do we need to look at regulation, governance, or whatever version of that we come to in the end, in the design of services?

Mark Bunting: The interesting question is about the process that intermediaries have gone through in designing new services or features. I would be very cautious in specifying rules about what design features platforms must have, or the particular tasks that they have to incorporate in design processes, but there is the concept of responsible design, which I think is partly what you are alluding to. For me, the interesting part of that is whether intermediaries, in designing their platforms, have taken reasonable steps to think about what the unintended consequences of those design choices might be. Have they been open and accountable in deciding what to do about those unintended consequences?

To give a practical example, the chief executive of Instagram has been very public about his attempt to shape the Instagram environment in a way that makes it harder for trolls to abuse people on that platform. That was partly for commercial reasons, because a clean environment is one that people want to spend time in, but there was also an ethical dimension in the way he talked about it. There were choices that he could have made or not made. We want to try to find ways of encouraging platforms to have design processes that enable them to think about those sorts of consequences, and make choices about them ahead of services being launched, rather than waiting for problems to emerge later.

Viscount Colville of Culross: How would you suggest doing that?

Mark Bunting: It is probably hard to avoid coming back to codes of practice and statements of principle. For example, there could be a code of practice that specifies the sort of external third-party engagement platforms might be expected to have in their development. There is expertise in the effects of technology on products. Have platforms taken reasonable steps to understand that research and evidence? Can they demonstrate how they have taken it into account in their design choices? You can set general expectations of engagement and anticipation of potential problems without necessarily specifying in great detail actions platforms should undertake.

Dr Damian Tambini: There is a slightly more direct and less hedged way of answering the question. How would you get them to do what you want them to do, or what the public want them to do? In general, we need to tread very carefully, because there are issues of media independence and the autonomy of those organisations from the state wrapped up in any of the moves that are made. There is a wider bundle of issues in platforms developing their ethics. This is an example of them developing their ethics and sense of social responsibility in a dialogue with society through institutions such as Parliament.

It is not the case that there are no levers in the hands of Parliaments. We could consider this a historical moment. There are historical moments when companies become too big and powerful, and they are regulated as monopolies. If that does not work, they are broken up. In a sense, Mark’s buckets are, unfortunately, overflowing into one another, because that is when the question of competition runs into all these other questions. If in five years’ time this and other Committees are still aware that there is a significant consumer and citizen detriment in relation to the platforms, other things—taxation, competition law and changes to the regulatory framework—might need to be brought into play, so there is a big stick in the background.

Baroness Kidron: Dr Tambini, as you are being very direct, there are not only unintended consequences of design but intended consequences of design, which I think was what the previous witness was getting at. We have design based on addictive loops. In your direct answer, would you say that is something one should look at in a societal way, whatever the framework?

Dr Damian Tambini: As a personal view, I think that is an issue, and it is coming out of the research, whether it is research on children or on social media use more generally. As a policy expert, I am quite intrigued by the question of how we have that conversation. Institutionally, something is not quite working when a moral panic blows up, and Select Committees are asking for the removal of certain kinds of content. We have small moral panics and we do not have an effective regulatory process whereby there is clear articulation by public authorities of what the ask is, with the clear involvement of civil society and the public.

At this point, I have to raise a question for the Committee about something I have attempted to look at as a private citizen. What is happening with the digital charter? Is that such a process? There does not seem to be a huge amount of transparency to the public. I tried to find out what was happening. How legitimate can that process be if even experts do not know what is going on with the digital charter? Historically, those kinds of processes, such as the royal commissions on the press going back to 1947, have tended to be cross-party and appointed by Parliament, but they involve other parts of civil society and are utterly transparent.

Baroness Bertin: I should declare an interest: I work part-time for BT. You talked about breaking up monopolies. I would love to know how you think the break-up of Facebook, for example, could realistically work.

Dr Damian Tambini: Obviously, this is different from how BT is regulated, or from the historical break-ups of telecoms monopolies that were in one country. We are in uncharted territory, but services provided through specific markets such as advertising, in which these companies are operating, could be separated through obligations that they are, for accounting purposes, separate from other divisions within the company. This has only relatively recently been on the agenda, so I posit it not as a fully developed policy design but as an idea.

It would be difficult, with the possibility of companies such as Facebook, Google or others withdrawing their services from a particular market. They have done that in certain instances where regulatory burdens were inappropriate, whether that is China or Spain. Certain services were withdrawn. I absolutely take that point. Effectively, a regulator working within one market cannot break up Google or Facebook globally, but it can enforce certain kinds of accounting separation within their operations in this market.

Baroness Bertin: I am not dismissing the idea; it sounds really interesting.

Baroness McIntosh of Hudnall: I want to go back to the issue Baroness Kidron raised about design to try to tie it to the point Mr Bunting made about a values base. Are there any models outside media, not necessarily specific regulatory models, to which we could look for ways of thinking about harm and that we could apply to the question of design? For example, nobody thinks it is a bad thing that there is no lead in the paint on children's toys. Once upon a time there was, and it had to be regulated away; people were not allowed to sell toys if they had lead paint on them. There may be something in that area. It is not to do with the content. A toy could be in many different shapes and sizes and intended to do many different things, but if it had lead paint it could not be sold. Is there something about design in other kinds of regulation that can be viewed in that way and drawn into this discussion?

Mark Bunting: I might give you a yes or no answer. Last week, you had before you Lorna Woods, who is working with Will Perrin. They are exploring whether there are analogies with workplace safety legislation, which is quite an attractive analogy. Workplace safety legislation is not so much about specifying that there have to be so many fire exits and this kind of smoke alarm; it is more a general principle that workplaces should be safe places in which to operate, and then it is up to companies to work out how to do that. That is potentially quite attractive.

The limiting thing, which is where the "no" part comes in, is that I am not sure we yet have a very good grip on the range of potential problems we might be dealing with. In workplaces, by the time the legislation was passed, we knew what sort of industrial accidents happened, and companies could be reasonably well placed to develop policies to address them. In this climate, we do not necessarily have a very good picture of exactly what the problems are, or how to identify them when they arise. That is not to say that the analogy does not work, but that we almost need to take a step back and find ways of engaging with companies about the actual risks associated with their products, and somehow incentivise them to have an open conversation about that, including, as Damian says, civil society and other stakeholders. That is a very difficult task, but it seems to me that in a way it is the heart of the regulatory challenge.

Baroness McIntosh of Hudnall: It may be difficult, but it is not unprecedented. That is all I am trying to inquire about. Is that right?

Mark Bunting: In broad terms, I agree.

Dr Damian Tambini: To extend the analogy, if the toy is an online game, one of the problems is that "Grand Theft Auto" may be bad for children, but a number of adults will think it is their right to use it, so you cannot simply remove it from the market.

Closer to home, there are some interesting analogies in how these ethics emerge. Even in newspapers, the separation of editorial from advertising and the separation of comment from factual reporting emerged, and they help consumers to know where they are and they protect democracy. The question is how to have conversations about how that ethic works and how it is communicated to a very confused public.

The Lord Bishop of Chelmsford: I want to take you back briefly to your very first answer to Baroness Kidron's question about whether it is a publisher or platform. I am still not convinced by your answer. I understand that it is not a publisher as we understand that word, but neither is it a platform in the way I think most of us understand that word. It likes to present itself as a library. When I go to the library, it is a democratic space where every book is equal, and to navigate my way round the library I have to work out the index system.

It is not like that; it is like going to WH Smith, which I thought was a stationer or bookshop, but now, when I go to the till, I am bombarded with all the other stuff they are trying to sell me. Do not tell me it is just a platform. I wonder whether we need some new language, rather than just sitting behind the old language. Maybe one of the things we could usefully do is to ask whether there is a new way of defining what that space is. That might be the key to unlocking how we might do the things I think we all want to do.

The Chairman: Do you think that is something the Committee could usefully do?

Mark Bunting: Yes, but I urge you to focus on the activities that are causing harm rather than getting too caught up in the definition. I agree that, for example, Facebook is neither a straight publisher nor a straight platform, but there are many different companies in this space with very different business models that operate in different ways.

One of the regulatory tasks is to find a way of capturing potentially everybody from Google Search at one end, through Facebook—they are two very different services but they tend to get bundled together—all the way down to much smaller sites that may have a particular task; for example, sites that enable teens to upload videos about their homework may have particular obligations. They may not look the same on the outside, but they manage, or curate, our access to content, which is of vital importance to fundamental rights. To my mind, that is the activity we need to find ways of engaging with.

Dr Damian Tambini: I agree. You put your finger very neatly on the challenge, which is to come up with definitions that people generally understand and find intuitive, but which also represent in some way how the regulation and the institutions are working.

To come back to my original point, legally, platforms are not liable for content that they do not know about. That is the key thing. The way that people use platforms such as Facebook and others has more to do with the way they understand television and media historically. There has always been a slight catch-up in media literacy and people's understanding of the risks associated with the environments in which they find themselves.

Q14 **Viscount Colville of Culross:** We have talked a little bit about regulating content. I would like to ask about the way platforms moderate content and whether it is fair and transparent. Mr Bunting, you have written about accountable design for algorithms. Is that something we should be looking at? We keep hearing about algorithms and the way they drive users in certain ways. Is that an area we should look at making more transparent or, if that is not possible, persuading platforms to make it more transparent? Should we be getting involved in that area?

Mark Bunting: I think you should. To my mind, the concept of accountability in algorithms is more important than transparency. Another way of putting it is that it depends on what you want them to be transparent about. I do not think that transparency of an algorithm in itself means very much, because they could publish the billions of lines of code that make up the algorithm and none of us would be any the wiser.

The aspiration would be that we know a bit more about what the algorithms are trying to solve and what are the data on which they have trained those algorithms. For example, if there is an algorithm to detect extremist content on YouTube, my question would be, "YouTube, what have you done to assess whether that algorithm is working effectively both in capturing content that genuinely is extremist when qualified people look at it, and in not capturing all sorts of material that is legal content and has just inadvertently fallen foul of an algorithm?" It is not the algorithms themselves that policymakers should be exercised about; it is the steps platforms have taken to ensure that the algorithms are working as intended, and how they are measuring success and reporting it against those objectives.

That is a legitimate question, partly because the platforms have said that they now do a lot using automated tools to detect all kinds of illegal material, but they do not say very much about how they have evaluated the effectiveness of those automated tools. Finding ways of incentivising platforms to adopt principles of good governance, accountability, openness and impact assessment is the most important task.

The Chairman: Do you agree, Dr Tambini?

Dr Damian Tambini: It is important to open it up a bit. There is the general process of curation, which includes the positive promotion of certain kinds of content, and may be done by the special source relevance algorithm on any platform. There is also a narrower category, which is the removal of content that breaches community guidelines or the law.

In relation to the second category, people very often categorise the platforms as censors, and campaigners and policymakers are keen to point that out. They say that taking down material impacts fundamental rights, so it should be subject to due process and appeal, and opportunities to put back content. Then you get into questions about scale and practicalities. The platforms say it is very difficult to scale, because they do a lot of it automatically and with low-paid moderators. There is thus a practical problem that the big platforms in particular have something like a censorship role, and policymakers and others do not quite know whether they are editors or censors. That is a really important principle to take into account.

When we come back to the question of competition being linked to content regulation, the principle is important. A platform that does not have very many users and has a small market is much more like a publisher, a journalist or an editor. On the other hand, a platform with a large market share is operating something much more akin to a censorship role, whether that is taking down content or the right to be forgotten or impacting on fundamental rights in another way. What we do not have in the regulatory framework is the possibility of linking regulatory obligations to size. That goes across many different areas. One of the institutional issues we pointed out at the beginning is how to have some kind of regulatory institution that is able to link those competition and other public policy issues.

Baroness Kidron: I want to go back to the issue of responsibility. Mr Bunting, you have referred a couple of times to the intended consequences, or the idea that there is only deliberate good happening, and you, Dr Tambini, have just referred to low-paid workers. That is a choice, too. Everybody wants this technology to be wonderful, accessible and available. That we are all agreed on, but we are trying to imagine another world where the status quo is not automatically assumed. They could have high-paid workers who might have more skills. I am interested in responsibility. Regulation is not the only tool in the shed.

Mark Bunting: On issues such as labour rights and employment conditions, those firms should be held to the same standards as other firms. To the extent that there is regulation of international labour rights, of course they should apply equally, and there are processes in place to enable investigation of those things.

I hesitate slightly, because I feel that sometimes we are at risk of holding these companies to a higher standard than we would have held companies in the past. The companies have a very strong incentive to maximise their value to users, and I take the point that that can tip over into addictive behaviour. Where there is robust evidence that products are addictive, there is a role for regulation, in the same way as there is for gambling and alcohol. I do not know enough about the area to know how conclusive the evidence is at this stage, but we should be careful not to detract from the value of platforms for the majority of their users because of concerns about a minority of users who may be using them inappropriately. There is a balance of responsibility between the users themselves and the platforms.

Dr Damian Tambini: I agree with my colleague about labour rights; other aspects of what the platforms do are effectively regulated in other ways. I am arguing that perhaps we need some sort of new institution, even a regulator, but we should be wary, because one of the arguments against that is that it will be a Christmas tree. Everyone will hang on their pet issue, so anything that is done needs to be very closely circumscribed and not to overlap with other issues.

Q15 **Lord Gordon of Strathblane:** What role can users play in establishing and maintaining online community standards other than simply boycotting the service and hitting the share price of its provider?

Mark Bunting: There are a few ways. The most powerful way is as a user of the service. One of the things that platforms do very well is fine-tuning the way they operate to try to ensure that they deliver a service of value to users. There are some suggestions that Facebook’s growth may be slowing; usage is declining in some markets. It is impossible to know the extent to which that is to do with some of the public issues that have arisen over the past few months, but if users feel that the platform is not operating effectively for them they will go elsewhere. That was how Facebook came to replace Myspace in the first place, so that is important

Beyond that, there have been efforts, particularly by Facebook, to consult users on changes of policy and terms of use, although they have been somewhat variable over time. This morning, I happened to look at the Facebook governance page, as I think it is called, which has had a recent update of its data policies. The previous update was in 2015, so perhaps the engagement is not quite as frequent as we might like.

The third area, which in a way comes back to the point about design, is that users play a very important role in establishing the norms of platforms.

Lord Gordon of Strathblane: But do they? Surely, it is just signing up to the terms and conditions, and those are devised by the platform provider.

Mark Bunting: They are. Clearly, they are very important rules and documents, and the power of algorithms in shaping the ways we interact is greater than the ability of users to force change. Part of what we are seeing is a gradual evolution in people's understanding of the right and wrong ways of using services. It is a slow process, and it is not as rapid as the platforms changing themselves, but users have a role to play in helping to set norms, and platforms have a role to play in trying to enable the formation of norms that are more responsible rather than more damaging.

Lord Gordon of Strathblane: I do not think anyone would accuse platforms of encouraging violence, but they certainly seem to enable it. People who one hopes would behave perfectly properly if they met somebody in the street behave like absolute morons online. Is there some work being done on that?

Dr Damian Tambini: It has been widely recognised that there is what Michael Ignatieff calls digital disinhibition. Other than that, there seems to be a pattern that people are much less inhibited, and the usual social norms do not restrict behaviour.

Going back to the question about what users should do, I agree; they should switch. They should be able to switch between platforms. One of the problems, which is linked to some of the competition issues, is that there is quite effective consumer lock-in for reasons of data portability, barriers to entry and the costs of switching. Those appear to be very high, which is a competition policy issue in itself.

Many users are children. There are specific issues around how the process of learning works between children, parents, schools and platforms. It is very much fits and starts. One of the reasons is that different platforms have very different approaches to children, whether that is consent age to join the platform and how they are treated for data protection purposes, or content moderation standards. They all have very different policies. That creates difficulties for parents and schools in working out appropriate rules for children and effectively communicating them, which is an area that I think the Government are looking into at the moment.

Q16 **Baroness Bertin:** My question is about balance in online protection, child protection and hate crime. How do you get the right balance? It is such a grey area—not child protection—but I would like to have your views as technical experts about how realistic you think it is to put the genie back in the bottle.

Dr Damian Tambini: It is very difficult to get the balance right. It is a question of procedures. How do you create a pyramid whereby complaints and disputes that are clear and easy to deal with are dealt with by the platforms at a low level, with the potential to escalate to a co-regulatory body and ultimately, for a very small number, to the courts in setting standards, if that involves illegal content? The challenge is to come up with effective procedures.

The German hate speech law, for example, which has been much commented on, is controversial because it is seen as an infringement of free speech rights. It establishes a procedure. In Germany, as here, authorities were getting impatient with platforms being very slow to take down hate speech, harassment and violent content that was illegal and breached German law. They set in law clear guidelines for different categories of content. It needs to be taken down within 24 hours if it is clearly infringing the law, and within a longer period if it is more difficult to categorise. A small number can be referred to a publicly appointed board if they are too difficult to deal with and the platforms cannot reach a clear view on them.

There are possible procedural solutions, but it is a question of getting the balance right in how much you push back to the platforms to adjudicate those rights and where the rules come from. Should the rules be set by Parliament or by the platforms? Should consumers have the ability to switch on the basis of different policies, or is there some other model? At the moment, there is a bit of confusion.

Baroness Bertin: We know there are millions of child images at the moment. Do you think companies could do more to stop those images going on to platforms in the first place? I think they are hiding behind, "We have referred thousands of these images to the authorities", but that clogs up the whole system, and one could argue that in some ways it is not helpful. They need to stop the images going on there in the first place. Do you think they could move more towards that?

Mark Bunting: There have been moves towards that. Collaboration in that area goes back a long way, as you may know through your BT relationship. The Internet Watch Foundation was established as an industry body in the 1990s, under very significant political pressure and the risk of regulation, to try to find ways of dealing with those sorts of problems. Initially, it very much involved that sort of notification and action, but BT was very active in developing technological solutions to enable ISPs to identify flagged content. The question of whether that is enough and whether more can be done is virtually impossible to answer without being much closer to the detail.

Baroness Bertin: You mean the technological detail.

Mark Bunting: Yes, but also evaluations of the effectiveness of what currently takes place. To touch on a point we made earlier, there is not a huge amount of external accountability in these areas, in the sense that those sorts of evaluations and assessments of what more could be done are generally not publicly available. The answer to your question is, "Possibly", but it reveals a broader issue, which is that there is expertise working very hard on those questions, but we find it difficult to hold the activity to account and understand how effective it really is.

Q17 **The Lord Bishop of Chelmsford:** I want to focus on what is often referred to as the TV-like content that now appears on the internet in video on demand. A couple of years ago, the authority for television on demand shut down and its functions are now with Ofcom. I have two questions. How should we regulate video-on-demand services, and who should the regulator be? Should it be Ofcom, or do we need a new regulatory body specifically designed to regulate this sort of content?

Dr Damian Tambini: We are in a period of transition. In the past, obviously anything that was TV-like required spectrum for broadcasting and was licensed. In the future, just about everybody will be providing video and it will be much less regulated. We are somewhere in between, where there are categories of TV-like content. That is why in the audio-visual media services directive a specific package of very basic rules applies to that category.

Consumers are catching up. They expect on-demand platforms to be less regulated than broadcast platforms. There seems to be a space emerging for a co-regulatory body with multiple roles, including auditing various forms of editorial content online. It may be an on-demand regulator, in the sense that platforms ask to be regulated by it. There may be a voluntary aspect, but I would not base it on any type of content or medium of delivery. That would be a mistake, given the rate of change. We need a system based on opt-in or services such as news versus other kinds of service, rather than types of service as in video versus radio or text.

The Lord Bishop of Chelmsford: You said that the viewer has different expectations. I am not suggesting that you are wrong, but I would be interested in the evidence for that. People increasingly receive all these things through their smart TVs. Do they have different expectations, or do they just think, "I'm watching TV"?

Dr Damian Tambini: You have caught me there, because it is some years since I looked at the evidence. Ofcom surveys these things annually in terms of consumers' expectations. This is going back a long way to the time I was involved in setting out policy before the Communications Act 2003. That was done very much on the basis that consumer expectation at that point remained that video platforms, TV and TV-like content would be regulated. That was where consumers were. I am offering my judgment and estimate, and the Committee should probably look at the evidence, but my sense is that consumers, particularly younger people, have moved on considerably.

The Lord Bishop of Chelmsford: I am sure we got it from Ofcom, but it would be worth looking at it again. Thank you.

Mark Bunting: For me, the big distinction is not between broadcast TV-like services and online TV-like services but between commissioned and editorially controlled services, in which I would count Netflix and Amazon as much as I do the BBC, and open video platforms of the likes of YouTube. Historically, YouTube has not been in scope for any of this regulation because it is not a TV-like service, although there is some debate in the AVMS directive review about what obligations platforms such as YouTube should now be subject to.

In the former category, the Netflixes and Amazons, personally I do not see a strong case for changing the current regulatory regime. The rules for those services are broadly similar to those for broadcast services, and Ofcom has responsibility across the piece. If we move beyond the current regulatory requirements and think about how to regulate YouTube, it will be a very different kettle of fish, and all the issues we have been talking about today will come home to roost. There is a separate question about what role Ofcom should play, and whether a new institution is needed for that.

Lord Gordon of Strathblane: Concentrating on the services that are like television, is there a case for making the regulation identical? I thought that might be the implication of what you were saying. In which case, do we end up regulating online as we do offline at the moment, or do we deregulate offline to the equivalent of what online has become?

Mark Bunting: Personally, I do not think that the principle that the same rules should apply to everything is necessarily a useful starting point because of Damian’s point about how expectations may or may not vary. I do not know the answer to that question. To the extent that audiences have different expectations of Netflix or Amazon, there would be a reason for having different standards from those that apply to, say, the BBC, but that is an empirical question. I do not think it is one where you would start from the principle of saying that the same should apply across the piece.

Dr Damian Tambini: To underline that, Mark has advanced one idea of what should guide regulatory design in editorial control, but I want to return to the point I made previously about size. These are not rules that should apply to every publisher, including the Facebook accounts of everybody in this Room. The rules should apply potentially to large and powerful companies that have a huge impact on our national life.

Q18 **The Lord Bishop of Chelmsford:** What do you see as the future role for public service broadcasters? Netflix will be spending $8 billion on content this year, and the BBC will be spending £1.6 billion. The big are getting very, very big, and one wonders what the future is for PSBs. Do you have any thoughts on that? What might regulation do to help that economy of broadcasting?

Mark Bunting: I can give you a brief and high-level view. Public service broadcasting continues to be very important, not only for the public policy and social considerations that weigh on policy-makers but because it still accounts for the majority of viewing in the UK. Despite the vast sums of money that Netflix and Amazon spend, they still account for a relatively small share of video consumption.

To go back to the previous question, it is right that we expect a different level of commitment or obligation from public service broadcasters than we would from purely online services. The key question is funding and the sustainability of the obligations that they face. I am not in a position to give you a view about how sustainable those obligations are, but you can see risks coming down the track. It is not just about content competition; it is about competition for advertising and talent. In those areas, all the PSBs find life harder than they did in the past. Parliament, the Government and Ofcom all have important roles to play in monitoring the health of that ecosystem and trying to find ways of propping up what continues to matter.

Dr Damian Tambini: The Committee should not miss the opportunity to mention the importance of the security of BBC funding and of independence protection in the process of review of BBC funding, which was a serious problem in the last funding rounds. We need to avoid that happening again.

As the focus is on internet platforms, the issue of prominence and findability is hugely important. It would be interesting to think about that if one of the things the Committee is doing is trying to articulate the beginning of a societal ask of the platforms. They develop algorithms to make certain kinds of content prominent; for example, Facebook is discussing how to develop in the United States a way of recognising quality news. It is also looking at crowdsourcing through user recommendations and surveys, and a way of bumping certain quality services up the news feed.

That is hugely important after the recent emergencies we have had about fake news and disinformation, and what the BBC is doing is more important than it has ever been. That activity on the part of the platforms should, surely, incorporate what Parliament and society have agreed is to be viewed as socially important quality content, which is funded and legally required to be universally available. There is an area around prominence and findability that needs to be worked into the framework.

Q19 **Lord Goodlad:** You mentioned transparency a short time ago. First, what information do you think online platforms should provide to users about the use of their personal data and how it should be presented? Secondly, do you think that the general data protection regulation provides sufficient protection for people on transparency in the collection and use of personal data, or do we need further regulation?

Dr Damian Tambini: The GDPR is definitely a step in the right direction. A lot will depend on how it is implemented. There is obviously discretion, with new legislation being passed here. There will also be some discretion in implementing it by the Information Commissioner’s Office.

A key area that I would like to highlight is data portability. One of the objectives of introducing data portability was to give consumers the ability to download their data to bring down switching costs so that they can move to other social media platforms. It is hugely important that that is effectively implemented, and that we develop common standards for the formats that will, effectively, feed into competition between social networks so that it is practically possible. It will be interesting to see how that develops over the next weeks and months.

There are difficulties with transparency when we are talking about privacy. In some ways, the principles have always been there, and some of the rules will not make a huge amount of difference. It may be possible that the Committee can help by making consumers and the public more aware of the rights they have. In a sense, it is too soon to tell.

Mark Bunting: I agree. I was just looking at some research that Doteveryone published recently that shows the limits to users' understanding of how data is used now. It found that 45% of members of the public were unaware that information they enter on websites and social media can be used to target ads; 32% do not realise that their search data is collected; and 30% do not realise that their purchase data is collected, so there is a significant comprehension gap. Mark Zuckerberg himself said at one of his congressional committee appearances that no one ever reads the terms of use and end-user licence agreements that they sign. At that level, there is common recognition of an issue.

What is unclear is how much users really care about privacy, whether they will change their behaviour as a result of more information becoming available, and, if so, how quickly those effects will work through. That remains to be seen, but it is at least possible that making more information available to users may not in itself do very much to ensure responsible use of data, which is where GDPR comes in.

Q20 **Baroness McIntosh of Hudnall:** This is a rather big question late in the day. You have talked quite a lot about competition law as we have gone along, and my question is about whether our current competition law is effective. Dr Tambini, I know from your evidence that you do not think it is, and that it is drawn too narrowly; you made some interesting observations about Amazon, for example.

Do you think that the law can be effective, or does there need to be new law to deal with the growth of platforms and their reach? Secondly, given that a lot of the current regulation is on a Europe-wide basis, what risks will we be exposed to in that area once we leave the European Union?

Dr Damian Tambini: The second question is easier. There are risks, if you crash out without a deal, that the rules are simply not clear, and there is a combination of directly effective EU legislation and domestically-passed law, with an unclear relationship between the two. There are also risks post Brexit of fragmentation, given that the Commission has in some cases been big enough to stand up to the legal power and expensive lawyers of the global giants in ways that may be more difficult for one country alone.

On the question of whether new legislation is necessary, there is an article by Lina Khan, a US academic, in the *Yale Law Journal* that I recommend to the Committee. She tells the story of how the enforcement of competition law and the tests applied by competition regulators in deciding whether there has been consumer detriment have changed in the last 20 to 30 years. She is speaking about it in the US context, but it also applies in Europe.

It would require some kind of legislative change to deal with the issue. Something could be done using the discretion of competition regulators post Brexit. Last week, Lorna Woods, one of your witnesses, referred to the Enterprise Act provisions on public interest in media mergers. In a merger situation, some kind of additional public interest could be taken into account by a Minister. That would not require new legislation; it would require some kind of clear signalling and clarification of the policy on the part of the Minister.

At the moment, in a merger situation, it is possible to have a reference to the public interest for almost anything that the Minister decides, but that requires merger rather than the organic growth of a company, which is very difficult for competition law to deal with. There are real problems, and legislation to change the Enterprise Act would be part of the solution. How the competition authorities advise Ministers on competition decisions and how they make their own decisions could also help.

Baroness McIntosh of Hudnall: You talked about the difference between merger and what you referred to as organic growth. The growth of these platforms has been to a large extent through the absorption of smaller entities, has it not? Start-ups have been sucked into the big platforms, and that is where a lot of their growth has come from. Do you think that in the application of competition law there is any particular advantage in the fact that their growth is not, as you make the distinction, organic in the usual way?

Dr Damian Tambini: Most of those mergers happen elsewhere in the world. In the case of the small number that occur in this country—I cannot think of a specific example right now—it is unlikely that they would meet the threshold required under the Enterprise Act for them to be referred to a Minister, so on reflection I do not think the legislation would be particularly useful in those cases.

One very interesting area in media pluralism, which has not come up yet but could, would be if a platform wanted to buy a broadcaster, for example. If a newspaper buys a broadcaster, there are special public interest requirements. If Sky wants to merge with another company, or have a change of control, there are broadcast licensing concerns, but those would not apply if a broadcaster was being purchased by a platform, rather than by another broadcaster or newspaper.

Mark Bunting: I have a slightly different view from Damian on the relationship between competition law and other issues. I certainly agree that competition law does not effectively address many of the concerns we have talked about. It does not have the tools to manage harmful or illegal content, addiction or any of those sorts of things. I agree with Damian that scale is very important. Having a regulatory regime that allows for differentiated responses to companies of different sizes is very important.

Where I would differ, in the interests of plurality in this session, is on the desirability of using competition law as a way of fixing issues of social welfare, in the sense of the externalities that we are dealing with. There are three brief reasons for that. The first is competence. Competition regulators find it hard to balance issues of social concern against competition. That is not surprising because it is very hard, but it is not clear that competition regulators are best placed to do that job. The second reason is to do with pace and reactivity. Competition law is essentially, not entirely but very often, an after-the-fact mechanism, and one of the things we want to try to achieve is a more forward-looking approach to some of the issues we have discussed.

The third reason is the most fundamental. It is not clear to me that the remedies of competition law really address some of the problems we are talking about, particularly in the area of harmful content, which is where I would be most concerned. They might make things worse by fragmenting the problem rather than consolidating it. Last week, I was at an event with Tony Curzon Price, who is now an economic adviser to the Business Secretary. He made the good point that content regulation has always relied on there being a good monopolist who can set standards across the whole of a sector. To the extent that competition law tends to be opposed to monopolists, those things cut against each other. My personal view is that you need different frameworks for different purposes.

Baroness McIntosh of Hudnall: You do not think that the addition of a public interest or public benefit element in the way decisions might be taken would go any way towards meeting your point.

Mark Bunting: I am open to being persuaded, but on the face of it, it seems hard. We currently have quite narrowly defined public interest grounds for intervention, and those have not historically been a recipe for rapid and clear decision-making processes. If we were to broaden them substantially and make them apply to a whole range of different conditions, we could find ourselves getting tied up in endless CMA-led processes and trying to reconcile very difficult issues about the balance between competition and the protection of children, or whatever it might be. That sounds as if it could be painful.

The Chairman: I thank our witnesses. We have a very broad inquiry, and you have brought us broad knowledge and expertise very early in our inquiry, which has helped us a great deal. Dr Tambini, you have sent us some very useful written evidence. We would welcome correspondence from you if you follow our work as the inquiry continues, particularly in the area of international developments. If you see developments globally that you think may be of interest and relevance to the Committee, we would very much like to hear from you. Thank you again for taking the trouble to come here today, and we hope to hear further from you during our inquiry.

Dr Rosie Campbell OBE, University of Leicester; Professor Teela Sanders, University of Leicester; and Professor Jane Scoular, University of Strathclyde – written evidence (IRN0017)

We submit evidence as researchers who have been involved in a three year study on the internet and sex work in the UK, funded by the Economic and Social Research Council. **Professor Teela Sanders, Dr Rosie Campbell OBE (University of Leicester), Professor Jane Scoular (University of Strathclyde).** Beyond the Gaze is the largest study to date of the safety, working practices and regulation of internet based sex work[513] in the UK. The aims of this research were to:

a. Understand the wider theoretical significance of new technologies for changing the social practice of sexual consumption and the sex industry.

b. Map the trends and understand the working practices in internet-based sex work markets within the broader processes of the regulation and policing of sex work in the UK.

c. learn how safety and health services working with sex workers have responded to the needs of this sector.

d. Facilitate the integration of online sex work into safety & health related provisions.

We use data here from the Online survey of 641 sex workers of all genders based in and/or working in the UK, who use the internet in their work. We also spoke to several key adult website platforms about the organisation of the sex industry online. Information is also provided from 16 police forces (56 officers)

Note the following

1) ***This is not a study of modern slavery and trafficking within the online adult sex work sector nor is it a study estimating the size of the online sex work sector generally, or the percentage of those within who are victims of modern slavery or are coerced.***

2) ***The sex industry is largely based online since the migration over the past decade, with a small street market, by comparison. The majority of online sex workers are independent self employed workers, who work legally alone.***

1. <u>Is there a need to introduce specific regulation for the internet? Is it desirable or possible?</u>

[513] The BtG definition of internet-based sex workers was: ‘Sex workers based on their own, or in collectives, or working through an agency, who use the internet to market or sell sexual services either directly (i.e. interacting with clients in person e.g. escorting, erotic massage, BDSM) or indirectly (i.e. interacting with clients online e.g. webcamming’).

Those involved in regulation of online platforms need to be aware that any changes to regulation, such as the banning of adult service sites or content, will impact on online sex workers directly and will undermine some of the beneficial aspects for sex workers of using these platforms, crucially for safety (see point 4) and independent working without third parties.

Amongst the police interviewed there was no support for outright banning of online advertising: The concerns raised by officers about prohibition were that this would;

- Make it more difficult to identify victims and investigate those who exploit sex workers such as organised crime groups committing modern slavery offences.

- Displace advertising and drive the sector underground, into the hands of individuals and organisations that were not visible legal companies, including organised crime groups, and possibly onto the dark net, making it even more challenging for police forces and more exploitative for sex workers.

- Reduce co-operation between sex workers, police and online platforms.

There's a danger of the more you legislate the more underground you drive it because, at the moment, traffickers will utilise these web services… if we can get to that information to safeguard people, then that's great. If we can create more legislation to naturally safeguard people without driving it underground, then that would be good… my fear would certainly be that if you legislate, then they will go onto less legitimate websites. (Police interviewee).

It's something that we can go on and look without causing any issue. What we don't want to do is for them to go to secret sites that we don't know about, because that's generally where the nasty people will go and look so they can't be traced. (Police interviewee)

These potential impacts were seen as particularly heightened with current limits to police resources and cyber skills capacity in contemporary policing.

Web companies interviewed also noted the problems of further regulation of online advertising, which did not take into account rapidly changing technology and, rather than preventing or addressing criminal practices such as slavery/trafficking would lead to '*more secrecy and… more danger to both parties'* (Moderator of online platform).

2. What should the legal liability of online platforms be for the content that they host?

   Support for more proactive measures by platforms to safeguard: representatives from several police forces felt platforms should be more proactive in measures to safeguard against trafficking, slavery & other forms exploitation. For example some police participants felt these platforms could do more to monitor the placing of advertisements to ascertain whether coercion might be involved. One police participant suggested it would be helpful if companies were more proactive and contacted the police if they had concerns about specific profile users, but it was also recognised there were data protection concerns and the companies had their own business priorities.

Discussions about the regulation of online platforms must take on board that thousands of independent voluntary sex workers use these spaces for their marketing and for safety. Banning online advertising for adult services or overly restricting content would undermine the safety, labour rights & level of control over working practices for online sex workers & create a more hidden online sector with further challenges for law enforcement.

Recent amendments to law passed in the US Congress in March 2018, in theory to address 'sex trafficking' the Fight Online Sex Trafficking Act (FOSTA) and the Stop Enabling Sex Traffickers Act (SESTA), make websites liable for what users say and do on their platforms. This is already having huge ramifications for US independent sex workers as platforms make changes in relation to adult commercial content prior to the law being enacted in 2019, this is seeing a range of detrimental impacts including damage to livelihood and safety. These have included; the closure of major platforms or areas of platforms where sex workers have advertised for reasonable prices e.g. Backpage and Craigslist, curtailing the income of sex workers heightening poverty with some unable to pays rent and bills. This has included changes to terms and conditions on some spaces which now prohibit sex worker peer support and information sharing vital for screening and safety. This has also meant health, outreach and support projects having to remove information and advice whilst they consider whether this would be in breach. Indeed in the UK not only individual sex workers but also sex work support and safety schemes are having to review their online content and data management, as some may be using platforms with US jurisdictions. Sex work support organisations and sex worker rights organisations in the USA predict; increased dependence on third parties including exploitative ones, an increase in street work, an increase in violence against sex workers, voluntary sex work moving into more illicit even less visible spaces (including the dark net) and making it harder for law enforcement to identify none voluntary prostitution and cases of trafficking. US academic researchers Professor Scott Cunningham et al (2017) have analysed meta data on the shift to online sex work in the USA and found a reduction in murder and other violent crime against sex workers, they recommended laws such as FOSTA and SESTA which would curtail online advertising and screening would risk reversing such trends.

3. <u>How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?</u>

This is relevant to sex workers in relation to 'doxing' and the misuse of their information such as images.

Crimes against online sex workers: 80.8% (n=518) had experienced at least one form of crime in the past five years. 62.4% (n=400) had experienced at least one type of crime in the past year. The average number of types of crime experienced in the past 12 months was three. **There were relatively high levels of digitally facilitated crimes,** persistent or repeated unwanted contact or attempts to contact though email, text or social media (65%) and threatening or harassing texts, calls or emails (56%) were most commonly experienced. As part of these, threats to 'out' people about their sex work and to 'dox' i.e. posting sex workers personal details online were common. Non-payment or attempts to underpay for services was also one of the key crimes experienced (53.8%).

4. <u>What role should users play in establishing and maintaining online community standards for content and behaviour?</u>

Safety functions, digital footprint advertising platforms: sex worker participants highlighted how advertising platforms (including market lead platforms) had important safety functions and many consciously used certain platforms because of these:

- Platforms were identified which enable sex workers to provide feedback following a booking which only other sex workers could read to ascertain if there were any matters of concern e.g. they had been pushy, verbally, aggressive or tried to remove a condom - all taken as warning signs for further problematic behaviour and precursors to other crime.

- Some platforms require customers themselves to register, sex workers were conscious that this left a digital trace which contributed to safety by a. The need for a digital trace signals to individuals that record is being taken, this may deter some individuals from causing harm b. Leaves a starting point should there be an incident or crime which could be utilised in investigations or used to warn other sex workers (e.g. a profile name on a certain platform). Sex workers were aware that such processes were not infallible, with the possibility of false or proxy registrations, but were part of the risk reduction safety strategies adopted. 'any client who contacts platform 1 is traceable to an extent, having to provide at least basic information to sign up and an IP can be tracked' (escort/cammer)

- Sex workers were also conscious of the creation of a digital trace via their pre booking communication in emails, mobile phone calls, SMS communications: this was something street sex workers (contact made face to face on street) and those working in parlours/brothels/walk up flats (where customers can turn up at premises without prior communication) usually do not have.

- Platform and self regulation: participants involved in web advertising platforms noted that there was a degree of self-regulation amongst platforms. They pointed to; terms and conditions, prohibiting use by under 18's, verification processes, promotion of third party reporting and safety schemes and cooperation with the police;

'We certainly self-regulate as a business and we work with the relevant authorities. We make sure nothing illegal is happening. We try to provide links to support services. We're available to talk. We're not hidden. (Interviewee in leading adult platform)

- Under-reporting of crime: only 23% had ever reported a work related crime to the police, 39% said they were very unlikely or likely to report a crime in the future, 28% were not sure, 33% said they were very likely or unlikely to report.

5. <u>What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?</u>

Safety benefits: the role of the internet in screening and wider safety strategies, particularly its importance for improving safety was a key finding of the BtG research with online sex workers. For three quarters of survey respondents it was reported as very important (47.1% n=302) or quite important (28.1% n=180) for safety. The main benefits to safety from using the internet related to;

- Being able to screen potential clients: 85% (n=545) of survey respondents felt the internet facilitated monitoring enquiries and screening clients, with sex workers using a range of screening techniques many enable by online and digital technology.

- Networking with other sex workers and health and support projects to access information to reduce risk and increase safety via sharing information and alerts about potentially dangerous clients through sex work forums, private groups and formal schemes such as National Ugly Mugs (NUM), and accessing safety buddies, was central to such networking.

6. <u>What information should online platforms provide to users about the use of their personal data?</u>

This should be upfront and transparent and reviewed regularly. For sex workers who are at risk of their images and information being taken and used by others maliciously and to significantly detrimental effects, platforms could be much more responsible in terms of their commitment to addressing sex workers needs and requests.

7. <u>In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?</u>

Not able to comment.

8. <u>What is the impact of the dominance of a small number of online platforms in certain online markets?</u>

- In the adult services website platforms there are some key players who some sex workers view as that monopolising the adult services profiles market. Whilst there are others (some of whom can be more communicable about their practice and responsibility). There are some disadvantages for sex workers that a significant proportion of adult services advertising is done through market lead website. Yet it is important to note some are satisfied with the services provided.

- Police interaction with online advertising platforms: many police forces represented had limited interaction with online companies, particularly as some are not UK-based which may complicate communication. While some police interviewees were familiar with and used specific links on major international platforms for criminal justice-related enquiries or reporting, it appeared others were not aware of such facilities. Some forces used certain major platforms to search for information, but many did not engage directly with the webmasters/administrators of these platforms, except occasionally in relation to specific operations. There were mixed reports on the response, with some participants finding varied cooperation. For example, one police interviewee commented on the experience of colleagues when running an operation: 'they contacted some of these companies and they said some were really helpful, others were, "It's got nothing to do with you".' However, others reported a more positive experience with good cooperation:

I found [a major online platform] very helpful…They came back in a really timely manner with the information that we needed … we were are able to progress because it was a safeguarding issue, the one that I'm thinking of, involving young people –no issues at all, found them very helpful. (Police interviewee)

Platforms and cooperation with the police: Online marketing platform representatives interviewed emphasised that where there were legitimate concerns about criminal activities, including human trafficking, child exploitation or coercion of adults, they were diligent in helping with enquiries: 'it's a perfectly legal business, we operate within the law and … our relationships with the police are very important'. This was also noted by an interviewee in a UK-wide online advertising platform, who stated they would cooperate with police requests: 'if it's a reasonable request, it sounds legal and proper'.

9. What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

   Not able to comment.

10 May 2018

CARE – written evidence (IRN0024)

<u>About CARE</u>

1. CARE (Christian Action Research and Education) is a well-established mainstream Christian charity providing resources and helping to bring Christian insight and experience to matters of public policy and practical caring initiatives across the UK.

<u>Executive Summary</u>

2. CARE believes that although the internet can provide an array of benefits and opportunities for children and adults. It can also pose some very serious risks. CARE's focus is on safe access for both children and adults. We are especially concerned about:

   - protecting children from accessing (whether deliberately or unintentionally) inappropriate, sexualised/pornographic material and the impact this has on them;

   - protection, in relation to online gambling – for children and for adults, when needed; and

   - the <u>outstanding</u> issues that arose from the debates on the Digital Economy Bill – how adult pornography is regulated online and what access can be made to child sexual abuse images and violent pornography behind age verification.

3. CARE believes that regulation of the internet is justified to **promote well-being and human dignity; and reduce the potential for it to cause harm.** Our submission focuses on Q1 and Q7.

Q1: Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

Consistent approach online vs offline

4. The Internet is a key part of the lives of adults and children. As this amazing technology has developed, CARE has argued for regulation that ensures children and adults stay safe. We agree with the Government that "*what is unacceptable offline should be unacceptable online…we expect standards of behaviour online to match those offline*". However, we are concerned that other statements in the Internet Safety Strategy Green Paper (hereafter the "Green Paper") may conflict with this principle: [514]

[514] Department for Digital, Culture, Media and Sport, Internet Safety Strategy Green Paper, October 2017, pages 7, 8 and 14 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf

- "*We also recognise that no technology can be inherently good or bad. We value a free and open internet that protects freedom of expression and the platforms that promote it. What matters are the choices that we all make when we use these tools, the support and education that is provided, and the way these relate to the values we share as a society*";

- "*We are clear that our support for a free and open Internet remains undimmed, and that we do not want to restrict access to the Internet*" (page 14)

These statements can be a carte-blanche for "anything goes". Indeed, without the sort of regulation that has recently been introduced by Part 3 of the Digital Economy Act (DEA) 2017, the internet becomes "the wild west". More recently, the Gambling Commission has produced proposals on regulation of online gambling **because** they recognise that there is potential for problems for problem gamblers which are unique to the internet (eg. Gambling being available 24/7 compared to the opening hours of local betting shops).[515]

5. CARE has previously argued that there should be a **consistent approach to regulating all media platforms** and that the Internet is no different in principle to any other media platform. For this very reason, we welcomed the Government's amendment in the House of Commons to the Digital Economy Bill to ensure that age verification (AV) for '18' rated material applied to on-demand programme services (now section 94). We were very disappointed that the principle of a common framework was not maintained throughout the Bill. This principle of a common framework was undermined by changes made at Report Stage in the House of Lords so that the standard of restricting so-called "prohibited material" was removed from content on the Internet but maintained for on-demand programme services in the Communications Act 2003 and video recordings classified under the Video Recordings Act 1984.

Pornography and other content

6. CARE has welcomed AV for access to online pornography but the Digital Economy Act (DEA) 2017 created a new threshold for what adults can and cannot see behind AV, different to that for other media platforms. The Government itself recognised the two systems are not the same: "*We are creating parity between the offline and the online worlds in protecting children from being able to access pornographic material. These are different and incomparable places, and this is* ***the closest we can get on parity of content*** *through the age verification regime*."[516] In the medium term, with the increasing predominance of the Internet, having a different regime for what is allowable behind AV online and offline, will be, as the Minister said in the House of Commons "*unsustainable*". [517] In a survey, 82% of the public

[515] http://www.gamblingcommission.gov.uk/PDF/Online-review-March-2018.pdf

[516] House of Lords Report Stage, 20 March 2017, col 38, https://hansard.parliament.uk/pdf/lords/2017-03-20

[517] House of Lords Second Reading, 13 December 2016, cols 1228-9, https://hansard.parliament.uk/pdf/lords/2016-12-13

said online standards should either be the same as those offline or even stronger. [518] We agree with the statement made by Claire Perry during the latter stages of the Digital Economy Bill: *"I have never understood why we should allow the internet to be a special form of content dissemination when we willingly accept self-regulation and Government regulation of other forms of media distribution*."[519] CARE believes that as well as introducing an "uncommon media standard", the resulting Act leaves loopholes:

- particularly that the extreme pornography definition is too narrow and ignores the evidence of the effects of violent pornography, which is contrary to messages on domestic violence, including the Prime Minister's initiative on domestic violence[520] and ignores previous statements by Ministers on links between violence and pornography[521]; and

- the fact that prohibited images of children (illegal material under section 62 of the Coroners and Justice Act 2009) are not excluded from what is acceptable to place behind AV.

7. We recognise that the Act requires a report on the operation of the definitions in Part 3 of the Bill, but this is not required until 18 months after Part 3 has come into effect. This means legislation will be implemented **positively facilitating adult access to non-photographic child sex abuse images,** including very life-like animated CGI images, and adult access to very violent pornography (albeit with the exception of the very most violent) for 18 months. The review will take months and if new legislation is to be introduced there will be a consultation and many further months during which the legislation goes through Parliament. In truth, even if the review decided to revert to the original definitions in the Bill to ensure that online enforcement standards meet offline enforcement standards, we will probably be looking at a 4 or 5 year delay which, given the nature of the subject matter, is completely unacceptable.

8. Furthermore, there is no-one responsible for ensuring **non-photographic child sexual abuse content is removed from the internet**. The latest CPS report on Violence against Women and Girls 2016-17 shows a continuing increase in the number of prosecutions for possession of prohibited images of children.[522] Yet this material is not part of the content that the age-verification regulator can require ISPs to block under section 23(1)(b) of the DEA 2017. Nor does it fall within the remit of the Internet Watch Foundation (IWF). The IWF states clearly on its website that for "non-photographic child sexual abuse content", it **covers content hosted in the UK only** whereas all other child sexual abuse content is assessed if it is

[518] ComRes interviewed 2,090 GB adults aged 18+ between 17th and 19th March 2017. ComRes is a member of the British Polling Council and abides by its rules

[519] Ping Pong in the House of Commons, 26 April 2017, col 1147, https://hansard.parliament.uk/pdf/commons/2017-04-26

[520] https://www.gov.uk/government/news/prime-ministers-plans-to-transform-the-way-we-tackle-domestic-violence-and-abuse

[521] https://hansard.parliament.uk/lords/2015-11-05/debates/15110533000335/Pornography#contribution-15110539000037

[522] http://www.cps.gov.uk/publications/docs/cps-vawg-report-2017.pdf, Table 15, page 40

hosted anywhere in the world.[523] In the 2017 IWF Annual Report, it states "*3,471 reports of alleged non-photographic images of child sexual abuse were made to us. None of these images were hosted in the UK, so they were not within our remit.*"[524] When the offence under the Coroners and Justice Act was introduced, the IWF made clear that they are unable to operate in partnership with other countries to take down these images as many countries do not have a similar offence.[525] **The practical outcome is that neither the IWF nor the new age-verification regulator has responsibility to ensure that this material is not accessible in the UK**. The Government did say at a late stage of the DEA debate that, "*Where material is criminal in nature and not hosted in the UK, the National Crime Agency's Child Exploitation and Online Protection Centre works with international partners through Interpol to address this material in that jurisdiction.*"[526] It is not clear how often this happens despite this material clearly being accessible in the UK as was demonstrated in *The Times* reporting of the material on Facebook in April 2017.[527] **CARE believes the loophole with respect to non-photographic child sexual abuse images should be addressed as a matter of urgency.**

9. The DEA AV provisions do not apply to social media, such as Twitter, but there are clear concerns about the content on social media (see our previous paragraph). Given the importance of the internet to children and young people, CARE believes that **parents should be assured** that social media sites (and other sites popular with children and young people) are committed to the safety of children and young people with requirements to tackle illegal content as well as objectionable behaviours. CARE was extremely disappointed that the scope of the Green Paper did not include illegal content[528] and believes that by not including *all* content that can be accessed on the Internet, the Green Paper's strategy is doing a disservice to users. While we welcome the Government's statement made in the House of Lords, that "*as part of the internet safety strategy the Government will work with social media companies to ensure that safety measures are built into online platforms so that parents can stay up to date*",[529] **CARE believes that parents should be assured that social media sites are protecting children and tackling illegal content as well as objectionable behaviours.** The proposed Social Media Code should be clear on the responsibilities of social media sites with respect to illegal material. The Social Media Code should be kept under review and if it does not respond to

[523] https://www.iwf.org.uk/what-we-do/how-we-assess-and-remove-content/laws-and-assessment-levels and https://www.iwf.org.uk/what-we-do/how-we-assess-and-remove-content (see Removing content in the UK)

[524] IWF 2017 Annual Report, page 15, https://www.iwf.org.uk/sites/default/files/reports/2018-04/IWF%202017%20Annual%20Report%20for%20web_0.pdf

[525] Evidence given to the Public Bill Committee, 3 February 2009, Q162, https://publications.parliament.uk/pa/cm200809/cmpublic/coroners/090203/pm/90203s07.htm

[526] Commons Ping Pong, *Op Cit,* col 1126

[527] Published 13 April 2013 https://www.thetimes.co.uk/edition/news/facebook-publishing-child-pornography-pdgt87nm6
https://www.thetimes.co.uk/article/face-facts-2zsrwt0wl and
https://www.thetimes.co.uk/article/facebook-s-darkest-secret-a-platform-for-paedophiles-hqlxxt2xq

[528] Green Paper, *Op Cit,* page 12

[529] Hansard, House of Lords, 7 November 2017, col 1671, https://hansard.parliament.uk/pdf/lords/2017-11-07

the concerns that have been expressed about content, the Government should consider introducing statutory regulation.

Family Friendly Filters

10. While the Government ensured that mobile phone operators and internet service providers (ISPs) **could legally provide filtering under EU net neutrality regulations** (section 94 of the DEA 2017), we remain disappointed the Government was not bolder in its support for parents and did not mandate that filtering be supplied as a default by Internet Service Providers (ISPs) during the Digital Economy Bill debates, even though it recognizes "*the benefit of current parental control filters*"[530] which had previously been described as "*a vital tool for parents".*[531] **CARE fully supports the recommendations on filtering made by the Select Committee's previous report on *Growing up with the Internet that "all ISPs and mobile network operators should be required not only to offer child-friendly content control filters, but also for those filters to be 'on' by default for all customers. Adult customers should be able to switch off such filters."***[532] If child protection is a high priority then the evidence that children will be kept safer online if filtering options are presented in the default-on format than in the unavoidable choice format must not be ignored**.**

11. We were disappointed that in the Green Paper and in the Government's response to the Committee's report,[533] the Government suggested that parents can apply "*filters where they are not engaged*", rather than advocating filters as part of parental management of online safety. CARE is also disappointed that the Green Paper states that "*A mandatory approach to filters risks replacing current, user-friendly tools (filtering across a variety of categories of content, but built on a common set of core categories) with a more inflexible 'top down' regulatory system*"[534] without citing any evidence or reasoning for this statement. Mandating that filters are introduced does not have to mean a uniform system for delivery

Gambling and children

12. **CARE is concerned that very young children are being targeted by gambling companies with websites that contain cartoon characters and free, or very lost cost, play;**[535] **and that these websites are able to circumvent legislation by claiming the sites are intended for**

[530] Department for Digital, Culture, Media and Sport, Internet Safety Strategy Green Paper, October 2017page 5

[531] House of Lords, Hansard, 5 November 2015, col 1799, https://hansard.parliament.uk/lords/2015-11-05/debates/15110533000335/Pornography

[532] House of Lords Communication Committee Report, *Growing Up with the Internet*, HL Paper 130, 21 March 2017, para 258 and 259, page 60, https://www.publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/130.pdf

[533] Lords Select Committee on Communication: Growing up with the Internet Government Response, October 2017, page 7 http://www.parliament.uk/documents/lords-committees/communications/children-internet/governmentresponsegrowingupwiththeinternet.pdf

[534] Green Paper, *Op Cit*, page 35

[535] The Times 8 October 2017, https://www.thetimes.co.uk/article/cartoons-lure-kids-to-online-gambling-vr6c83np6

adults. The Gambling Commission itself recently stated "*new technology is providing children with opportunities to experience gambling behaviours through products, such as free-to-play casino games, social media or within some computer games, which do not have the same level of protections or responsible gambling messages as regulated gambling products*."[536] In December, *The Guardian* reported on gambling apps that do not use money per se which can be accessed via Facebook without age verification checks.[537]

13. We welcome the Gambling Commission's proposal to consult on *"operators…providing greater protection"* for all those under 16, but it is not clear what this means in practice, especially as the concerns that the Commission has recognised also "*apply to gambling-style games that are offered by non-gambling operators (and over which gambling legislation and the Commission have no remit)."*[538] Furthermore there is a question about what protection is provided to 16 and 17 year olds. **Evidence suggests that "***there is an association between early gambling participation and problem gambling in adulthood*".[539] Professor Mark Griffiths, of the international gaming research unit at Nottingham Trent University has said, "*Research has shown that when we look at those children who are problem gamblers, the No 1 risk factor is playing games online for free*."[540] **CARE recommends that the Gambling Act 2005 should be amended to prohibit making online gambling games available to under 18s, even when there is no exchange of money**. The Act should be amended so that these sites should be subject to the Gambling Commission licensing conditions so that the same rules on advertising and age verification checks apply**,** with the same level of protections and responsible gambling messages as regulated gambling products**.**

14. **We also recommend that restrictions on the promotion of gambling to children should be included in the Gambling Commission's Licensing Codes;** in particular social responsibility code 3.2.11 should include the requirement to '*not deliberately provide facilities for gambling in such a way as to appeal particularly to children or young people, for example by reflecting or being associated with youth culture',* which already apply in the non-remote SR measures.[541] **It is indefensible not to include this requirement for remote operators, especially given the evidence above.**

15. CARE has also previously raised concerns about so-called "skins gambling".[542] In 2017, the Gambling Commission published the results of a

[536] http://www.gamblingcommission.gov.uk/news-action-and-statistics/news/2017/Children-experiencing-gambling.aspx

[537] https://www.theguardian.com/society/2017/dec/27/gambling-style-apps-offered-on-facebook-without-age-checks

[538] Review of Online Gambling, *Op Cit*, para 1.18(i)

[539] Consultation on proposals for changes to Gaming Machines and Social Responsibility Measures, *Op Cit,* **para 3.23**

[540] 8 October 2017, http://www.dailymail.co.uk/news/article-4961078/Online-bookies-use-cartoons-target-children.html

[541] See paras 3.2.1, 3.2.3. 3.2.7 http://live-gamblecom.cloud.contensis.com/PDF/LCCP/Licence-conditions-and-codes-of-practice.pdf

[542] "Skins gambling" is betting with in-game items when playing computer games or apps

question on skins gambling in its survey of young people's gambling habits, which showed that 20% of boys have said that they have been involved with "skins gambling".[543] They have also published their final advice on skins gambling; stating that, "*Where facilities for gambling are offered using such items, a licence is required in exactly the same manner as would be expected in circumstances where somebody uses or receives casino chips as a method of payment for gambling, which can later be exchanged for cash*" but noted that many of the sites are "unregulated".[544] However, these "unregulated" sites are **allowing children to gamble which is contrary to the Gambling Act 2005. Action to ensure these sites are licensed should be taken immediately**.[545] We are very concerned that while the huge problem presented by "skins" was noted in the Review of Online Gambling, **no specific action was recommended**.[546]

Q7. In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

16. **CARE agrees there is a need for transparency. Since our focus is on internet safety, in principle we support the Government's proposal for an annual internet safety transparency report.**[547] **However, in our view, it would need to go far wider than social media and cover:**

    - **what is and is not filtered by the Big Four ISPs who have a voluntary agreement with the Government and information on the filtering policy of all other ISPs servicing homes so that parents can make informed choices;** The current self-regulatory approach leaves big business deciding what is, and what is not considered 'adult content' to be filtered, rather than those decisions being made by a publicly appointed and accountable body. The Committee's previous reports stated that "*Parents and carers need clearly communicated information about the digital world*" and recommended that "*Those responsible for providing filtering and blocking services need to be transparent about which sites they block and why, and be open to complaints from websites to review their decisions within an agreed timeframe. Filter systems should be designed to an agreed minimum standard*."[548]

    - **information on the internet sites required to introduce age verification (AV) so that there is transparency about what websites are accessible only behind AV controls.**

11 May 2018

[543] Young People and Gambling 2017, *Op Cit,* page 5

[544] Virtual currencies, eSports and social casino gaming – position paper, March 2017, paras 3.8, 3.12-3.16, http://www.gamblingcommission.gov.uk/PDF/Virtual-currencies-eSports-and-social-casino-gaming.pdf

[545] Crackdown on gamers' gambling, Video game makers under pressure over 'skins' betting, *The Times,* 27 August 2017, https://www.thetimes.co.uk/article/crackdown-on-gamers-gambling-trl2dt7s8

[546] Review of Online Gambling, *Op Cit*, para 3.57

[547] Green Paper, *Op Cit,* **page 16**

[548] House of Lords Communications Select Committee, *Op Cit,* para 216, page 53 and para 259, page 60

CBI – written evidence (IRN0054)

1. The CBI welcomes the opportunity to respond to the House of Lords Communications Select Committee inquiry on internet regulation. We are the UK's leading business organisation, speaking for some 190,000 businesses that together employ around a third of the private sector workforce. Our membership is made up of businesses of all sizes, sectors and regions.

2. The UK is in an unprecedented era of change, from the digital revolution to Brexit, which presents new challenges for online business. The internet is already governed by a plethora of existing regulation that affects every business with an online presence. However, internet safety remains a pressing concern. Regulation can be a useful tool but other models, such as codes of practice and business initiatives, can be more targeted, proportionate and effective. Internet regulation must balance the multiple and diverse interests online - including online safety, intellectual property and innovation - all of which are vital for the UK's burgeoning digital and creative economies. Yet, there is still action that can be taken. Strong business engagement will be necessary to map current and future regulation and to highlight where and how gaps can be addressed.

3. The CBI urges the committee to consider the following recommendations on internet regulation:

    - Review the effect of current and forthcoming regulation, taking note of where businesses are already working towards self-regulation.

    - Maintain sustained and meaningful business engagement on the future of internet regulation, working collaboratively to identify gaps in regulation, deciding what the technological and non-regulatory 'art of the possible' might be and where there may be opportunities for further voluntary action.

    - Support businesses in continuing to develop codes of practice and implementing technological solutions such as automated detection technologies.

The UK has a unique, world-leading digital and creative economy

4. *One of the UK's greatest economic strengths is its internationally-renowned £170bn digital economy.*[549] The UK has a world leading digital sector, an exciting mix of home-grown entrepreneurial talent and international business prowess. Four of the five largest global investments in artificial

[549] TechNation Report 2017

intelligence businesses were for UK firms[550], whilst the UK is number one in the world for e-commerce[551] and is Europe's largest tech start-up hub.[552]

5. *And the UK's creative industries are producing world-class content to power the digital economy*. The UK is a global leader of creativity and provides an abundance of content that helps to power the digital economy. The UK's creative industries support two million jobs, contribute over £90bn to the UK economy, and were responsible for exporting over £20bn of services in 2015[553]. The sector makes a substantial contribution to the UK's cultural heritage and helps to project the UK's brand to audiences around the world. The UK's creative excellence has made it an attractive country for inward investment, and a centre for international businesses.

6. *Digital innovation is at the heart of economic, social and cultural development across the UK*. It drives productivity, generates investment, brings new products and services to consumers, creates jobs and raises living standards whilst laying the foundations for tomorrow's prosperity. And for many UK businesses, the internet offers the gateway to the digital economy, providing opportunities for new services, markets and disruptive business models.

7. *The CBI welcomes the government's continued support of the UK digital economy.* The government's Digital Strategy last year set out the UK's ambition to make every business a digital business, whilst supporting digital inclusion and connectivity across the country. The pioneering Centre for Data Ethics and Innovation will retain the UK's leadership in global data ethics debates. And most recently, business has welcomed the £1bn AI sector deal which embeds the UK's foundation as an international AI hub, and will be a powerful attraction for international trade and investment.

8. *Part of what makes the UK a success story in technology and digital is its innovation-friendly regulatory environment,* which attracts substantial international investment. And this regulatory landscape is constantly evolving. Today, businesses are improving data protection through GDPR, industry consortia are developing better self-regulation to combat illegal content online and the EU is introducing a new regulation on fairness in platforms-to-business relationships.

Now is a challenging time for business and regulatory uncertainty is already affecting investment decisions

9. *UK business faces great uncertainty, which is affecting investment decisions*. CBI surveys show that investment spending plans remain weaker than before the EU referendum, from capital to R&D. Over 40% of businesses have had investment decisions affected by Brexit.554 This is

[550] Atomico, The State of European Tech, 2017

[551] Centre for Retail Research, Online Shares of Retail Trade, 2017

[552] Startup Europe Partnership (SEP) Monitor 2017: https://mindthebridge.com/scaleup-uk-2017-sep-monitor-2017/

[553] DCMS Sector Economic Estimates 2016: GVA Report & Employment and Trade

[554] http://www.cbi.org.uk/news/brexit-is-affecting-investment-decisions/

creating challenging conditions for UK business. Further change in the regulatory environment risks adding to this uncertainty and affecting business decisions to locate or invest in the UK. As regulatory changes can add to the cumulative burden555 that online businesses face, **the UK government must ensure it gets the balance right between necessary internet regulation that solves a specific problem and over-regulation that stifles innovation and investment**.

10. *In March the Prime Minister noted that the UK would not remain in the Digital Single Market post-Brexit[556], but the UK will need to think carefully about how regulatory divergence impacts UK businesses*. The CBI's recent report, Smooth Operations[557], highlights the need for convergence on a range of EU digital policy regulations within the Digital Single Market. Regulation must be harmonised internationally to ensure that UK citizens can still access the benefits and services they do today. The CBI will be continuing to work with business to determine which digital policy dossiers are a priority in the future. When thinking about future regulatory responses, the government must also consider new EU legislation already coming down the pipeline and how these will affect the regulatory landscape.

Internet regulation already affects a plethora of businesses

11. *The world is in a period of digital disruption, but the internet is not unregulated. The UK has a complex web of internet regulation that affects all online businesses and many business issues.* The internet is governed by a range of existing regulation, including UK and EU law, codes of practice, and business initiatives. These cover an array of issues from copyright infringement to terrorist content and advertising. Figure 1 outlines some of the main regulations that businesses of all sizes are subject to online, as well as recent business initiatives and codes of practice.

12. *Internet regulation affects all businesses with an online presence.* It is not just platforms that would be affected by changes to internet regulations - a huge swathe of UK business would have to adapt, with some having more resource to do so than others. From a rural small business benefitting from the rise of online marketplaces, to a local news website with a comments section, changes would have far-reaching and potentially unintended consequences across sectors, and far beyond technology companies.

[555] http://www.cbi.org.uk/news/9-billion-a-year-policy-burden-could-weigh-on-businesses-ability-to-deliver-jobs-and-investment-cbi-director-general/

[556] https://www.gov.uk/government/speeches/pm-speech-on-our-future-economic-partnership-with-the-european-union

[557] http://www.cbi.org.uk/insight-and-analysis/smooth-operations/

Figure 1: Overview of the UK internet regulation landscape[558]

	Regulations	Description
Existing regulation	eCommerce Directive 2000	The eCommerce Directive places responsibilities on companies to remove illegal content online. It also provides specific and limited liability exemptions for businesses operating online; this is often called 'intermediary liability'. Businesses ('intermediaries') are not held liable for content that users produce, whether it be websites that internet service providers facilitate the connection to, or reader comments on news websites. As they host or transmit this content, rather than produce it, they are not liable. To keep their liability exemption, businesses must not modify this 'user-generated content' and must act quickly to take down or remove access to illegal content once notified of its existence. Online businesses have developed a range of notice and action systems to moderate content. These systems are in constant refinement. Newly proposed EU legislation would make these notice and action procedures more rigorous and transparent.
	Consumer rights	Both offline and online activity is also regulated by consumer rights, consumer protection and company law.[559] Businesses must ensure information about their products and services are accurate, transparent and treat consumers fairly. In the online world, consumers must know who they are transacting with and have a record of transaction terms. The Competition and Markets Authority oversees compliance with consumer protection laws.
	Sector-specific rules and enforcement	Businesses are subject to sector-specific rules and enforcement, for example, the Advertising Standards Authority rules on advertising breaches on online platforms[560], whilst the Information Commissioner's Office enforces data protection online.
	General Data Protection Regulation (to be enforced from 25 May 2018)	The GDPR is an EU regulation which represents the biggest change to data laws in over 20 years. The objective of GDPR is to harmonise the regulatory environment for data protection and enhance privacy rights for individuals. The regulation puts a spotlight on data protection for businesses and marks a positive step change in the level of accountability and transparency businesses will have to demonstrate in handling data.
Proposed regulation	EU platform to business regulation (April 2018)	This proposal from the European Commission aims to reduce unfair trading practices that harm business users of platforms.[561] The legislative proposal would increase transparency over delisting, terms and conditions, data access, and ranking criteria, whilst supporting better redress mechanisms for internal complaint handling and external mediation.

[558] This is not an exhaustive list but is intended to represent the diversity of internet regulation in the UK. Businesses are also subject to sector-specific regulation, for example in finance, medicine and retail.

[559] These include the Consumer Rights Act 2015, the Consumer Protection from Unfair Trading Regulations 2008, the Companies Act, and the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013

[560] For example, the CAP or BCAP Codes, which cover online advertising

[561] https://ec.europa.eu/digital-single-market/en/platforms-to-business-trading-practices

		An associated EU Observatory would monitor the legislation’s effectiveness and consider the need for future regulation.
	EU proposal to tackle illegal content online (March 2018)	This proposal aims to better tackle illegal content online. It involves increasing transparency on illegal content notification, fast-tracking ‘trusted flaggers’, and would require online operators to better inform content-providing users of moderation decisions and provide options to contest review outcomes. Companies would also be required to use proactive tools to detect and remove illegal content and better work with authorities in instances of serious criminal offence or where illegal content exposes a threat to life or safety.[562]
	Internet safety strategy and levy	The UK government is examining a strategy that considers the responsibilities of companies to their users and the use of technical solutions to prevent online harms. One major proposal is a voluntary Internet Safety Levy which would raise funds to tackle online safety issues. The CBI supports the introduction of an industry led, flexible levy which is targeted towards addressing clearly defined online harms.

	Initiatives	**Codes of practice**
Existing	The *Internet Matters* campaign aims to help make the internet safer. This campaign has invested millions in the past few years with the support of companies across the digital ecosystem and has had a demonstrable positive impact on improving safety standards.[563]	Voluntary *Code of Practice on IP infringement removal* (overseen by IPO)
	Get it Right from a Genuine Site is a successful copyright education campaign, organised through a partnership between government, BPI and the MPAA[564]	Voluntary European Commission *Code of Conduct against hate speech online*[565]
	Internet Watch Foundation[566] works with industry to make the internet safer by identifying and removing online images and videos of sexual abuse, using ‘image hash’ (digital fingerprint) technology	The *Sharing Economy Trust Seal*[567] is an example of an industry-led code which sets out clear standards of good practice for online platforms in a fast-growing and evolving sector.
	Global Internet Forum to Counter Extremism is an international forum encouraging social media sites to better remove radicalising and terrorist material online[568]	

[562] https://ec.europa.eu/digital-single-market/en/illegal-content-online-platforms

[563] https://www.internetmatters.org/about-us/impact-report-2014-2017

[564] https://www.getitrightfromagenuinesite.org/

[565] https://ec.europa.eu/unitedkingdom/news/big-tech-companies-quickly-remove-two-thirds-content-reported-illegal-hate-speech_en

[566] https://www.iwf.org.uk/

[567] http://www.sharingeconomyuk.com/trustseal

[568] http://www.bbc.co.uk/news/uk-politics-43944710

13. *For many businesses, today's internet governance regime has fostered a dynamic and prosperous online market.* For example, the eCommerce Directive (see figure 1) has given businesses the flexibility to develop new services that incorporate user experience, content and expertise, from the creation of online communities like Mumsnet and TripAdvisor, to product reviews on John Lewis' website and online forums on your PS4. This has allowed a great diversity[569] of individuals to connect, sharing content and experience in unprecedented ways, whilst supporting the UK's digital economy and enhancing prosperity. The eCommerce Directive has created the right conditions for start-ups and online businesses to enter new markets, internationalise quickly, foster new communities and provide significant economic and social value. For the creative industries, whilst the internet presents an opportunity to broaden the consumer base and appetite for British-produced creative content, it has also created revenue concerns due to copyright infringement.

The gaming industry

In the past, businesses sold video games on CD but now provide access to games that are hosted on online platforms. These platforms often include online forums and chat features, alongside access to search results that the games provider indexes rather than hosts, which fall within the liability exemptions within the eCommerce Directive.

A 'one size fits all' approach is not suitable for internet regulation; governance must balance a range of interests across different websites and issues. The outcome of internet regulation must be targeted, proportionate and stable.

14. *Internet regulation must balance complex interests between innovation, privacy, copyright, and transparency. Different approaches will be needed for different kinds of online illegal activity.* Internet regulation starts from the principle that if something is illegal offline, it is also illegal online – and this has widespread business support. As outlined in the government's Digital Charter, internet governance should be a delicate balance between addressing illegal activity in all its forms, protecting the privacy of citizens, retaining net neutrality and free speech, and nurturing the UK's digital and creative sectors. Further action is necessary to better remove illegal content online and keep citizens safe, but care must be taken to balance interests and provide solutions that work for different online problems. For example, changing internet liability is not a 'one size fits all' solution for all online illegal activity; it would have a wide-ranging effect on businesses. For instance – depending on how it is enacted - changing liability for an online start-up that hosts user recipes could limit business growth or viability; with greater liability risk and little resource to moderate content, the start-up may struggle between offering a service that their users value and remaining compliant with regulation.

[569] Ofcom Technology Tracker: https://www.ofcom.org.uk/__data/assets/pdf_file/0016/101293/technology-tracker-digital-participation-h1-2017.pdf

15. *The primary task must be to map the regulatory landscape and identify gaps:* Before any regulatory change can be considered, the regulatory landscape needs to be mapped out to determine where the precise gaps and issues are, and where business cooperation and non-regulatory solutions can be found. Solutions must solve specific problems and not cause unintended consequences for the wider business community.

16. *Progress on specific internet harms has already been made through voluntary government-business initiatives – both on copyright infringement and online safety. Voluntary business initiatives have a strong track record and the UK business appetite for self-regulation remains high.* Voluntary initiatives have been successful as they allow businesses to tailor solutions to their specific business models and requirements. Future internet regulation should take into account companies who are already investing in digital safety and copyright infringement improvements to ensure that existing campaigns continue to receive the best support. For example:

    - The European Commission's voluntary code of conduct for large technology businesses to combat the spread of hate speech online has been a resounding success. According to its most recent evaluation (November-December 2017), 70% of reported hate speech online is removed within 24 hours by business. 81% of this content is reviewed within the same timeframe.[570]

    - In 2017, a world-first *'responsible search' code of practice* was brokered between search engines (Google and Microsoft's Bing) and copyright holders to improve the takedown process for content infringing IP laws, as well as hate speech. The UK government's Intellectual Property Office played a key role in facilitating the process and continues to oversee the agreement.[571] To date, this code of practice has made significant progress in line with the metrics set.

Regulatory change is on the horizon; the impact of new regulations must be considered to avoid duplication or contradiction. The government should review the effect of current and forthcoming regulation, taking note of where businesses are already working towards self-regulation.

17. *The regulatory landscape is already changing. New regulation coming down the pipeline at both UK and EU level will fundamentally shift how the internet is governed and used* (see figure 1).

18. *Businesses have put significant resource into preparing for these changes, at high cost and regulatory burden*. The GDPR is a useful example of legislation that strikes the right balance in improving standards of protection whilst still enabling businesses to explore new products and

[570] https://ec.europa.eu/unitedkingdom/news/big-tech-companies-quickly-remove-two-thirds-content-reported-illegal-hate-speech_en

[571] https://www.gov.uk/government/news/search-engines-and-creative-industries-sign-anti-piracy-agreement

services. Yet, the cost of compliance should not be underestimated; the regulation took four years to develop, was the largest change to data protection in 20 years and involved extensive consultation and engagement across civil society and industry.

19. *The UK government should consider the effects of these changes in practice before enacting further regulatory change.* Regulatory changes such as the GDPR and the proposed internet safety levy, alongside emerging business practices, should be monitored and assessed to ensure that the current regulatory landscape remains fit for purpose.

20. *UK government's existing digital initiatives will also affect online businesses and their role in internet governance should be maximised.* It is likely, for example, that the AI Council and Centre for Data Ethics and Innovation will touch on the online use of AI, data protection and data ethics.

Future internet regulation should focus on government-business collaboration as well as non-legislative solutions. Continued monitoring of the regulatory landscape will help determine if further action is needed down the line.

21. *Whilst the internet is not unregulated, more needs to be done to strengthen enforcement of current law online.* Businesses understand the pressing need to better tackle internet safety and fairness online and have no interest in propagating illegal or unsavoury content. Businesses want to ensure that their services and business models are creating social, as well as economic, value.

22. *Action can be taken to support online businesses in their duty of care, without stifling innovation and rocking the foundations of the UK's digital and creative sectors.* Plenty more can be done through voluntary cooperation, alongside continued monitoring to determine if new regulatory action is needed further down the line. Businesses have a finite pool of resources to dedicate to getting regulatory compliance right, and therefore may need government support in terms of time, finance or convening power to ensure they can implement tailored solutions that work most effectively for their business models and customers.

23. *Businesses should continue to cooperate and collaborate on technological and other non-regulatory solutions, supported by government*. This includes:

    - *Developing better notice and action systems*: government should support businesses in enhancing and aligning 'notice and action' procedures. Work is already underway to make takedown notices more stringent, and the European Commission has made recent proposals in this area.[572] Supporting ongoing work in developing 'notice and stay down' systems would help address specific copyright infringement on some websites. This means that once an online business has been

[572] http://europa.eu/rapid/press-release_MEMO-18-1170_en.htm

notified of specific illegal files, the business will take all reasonable steps to ensure that all other copies of, or URL links to, the same illegal content are removed and do not appear on their websites in the future. Businesses are increasingly using and sharing technology that creates a digital footprint for illegal content, known as a 'hash'. This allows businesses to better scan for illegally-hosted content on their services.[573]

- *Continued government support of world-first initiatives and codes of practice and industry:* Much can be learned from the first government-led Global Internet Forum for Counter Terrorism which is leading the way in supporting social media sites taking down radicalising and terrorist material online.[574] This should pave the way for continued government-business collaboration within the remit of the Digital Charter.

- *Supporting further business-led practices:* To support online safety, many larger platforms are hiring thousands of new content moderators to increase the pace at which they can review user-generated content that contravenes their policies, and ultimately, the law. Businesses are also updating community standards and guidelines for content removal[575], publishing quarterly reports on enforcing community guidelines and providing information on user's reporting history.[576]

- *Supporting the use of automated detection technologies:* more work is necessary to support businesses in making the online world fairer and safer. A range of online businesses are starting to use rapidly-developing technologies like artificial intelligence to monitor content, which is having an increasingly positive impact. For example, 83% of the videos removed by YouTube last October were taken down before humans flagged them as inappropriate.[577] Technological solutions will need to balance differing interests and opinions online and incorporate appropriate redress mechanisms for wrong decisions.

[573] For example, the Internet Watch Foundation has an Image Hash List that uses 'hash' technology to scan for illegal and unsavoury photography on the internet, in collaboration with industry.

[574] As highlighted in Amber Rudd MP's resignation speech in May 2018: http://www.bbc.co.uk/news/uk-politics-43944710

[575] https://www.facebook.com/communitystandards/

[576] https://youtube.googleblog.com/2018/04/more-information-faster-removals-more.html

[577] https://youtube.googleblog.com/2017/10/an-update-on-our-commitment-to-fight.html

Automated detection technologies within industry

YouTube's *ContentID* scans uploaded videos against a database of files submitted by approved content owners (most often these are other companies). If a new upload matches an existing video, copyright owners can block the video or monetise it by running ads against it.

Google's incubator, *Jigsaw*, also uses rapidly-advancing technologies like machine learning to protect individuals from online harassment to countering violent extremism; the incubator has for example developed automated comment review for online news outlets.

Conclusion

24. The CBI has previously welcomed the aims of the government's Digital Charter to both increase public confidence and trust in new technologies whilst creating the foundations for the UK digital economy to thrive.

25. In conversation with industry, government must look at increasing public trust and transparency, whilst also supporting innovation-friendly regulation and considering the far-reaching impacts that changes to internet regulation will have for the entire UK business community operating online. This includes consideration of the delicate balance between innovation, liability, free speech, privacy and copyright. Any solutions to online harms must be targeted, proportionate and stable.

26. To that end, government should:

- Review the effect of current and forthcoming regulation, taking note of where businesses are already working towards self-regulation.

- Maintain sustained and meaningful business engagement on the future of internet regulation, working collaboratively to identify gaps in regulation, deciding what the technological and non-regulatory 'art of the possible' might be and where there may be opportunities for further voluntary action.

- Support businesses in continuing to develop codes of practice and implementing technological solutions such as automated detection technologies.

May 2018

Centre for Competition Policy, University of East Anglia – written evidence (IRN0020)

Authors:

- Dr Sally Broughton Micova, Lecturer in Communications Policy and Politics
- Dr Sabine Jacques, Lecturer in Intellectual Property Law, Information Technologies and Media Law

This consultation response has been drafted by the named academic members of the Centre, who retain responsibility for its content.

The Centre for Competition Policy (CCP)

CCP is an independent research centre established in 2004. CCP's research programme explores competition policy and regulation from the perspective of economics, law, business and political science. CCP has close links with, but is independent of, regulatory authorities and private sector practitioners. The Centre produces a regular series of Working Papers, policy briefings and publications. An e-bulletin keeps academics and practitioners in touch with publications and events, and a lively programme of conferences, workshops and practitioner seminars takes place throughout the year. Further information about CCP is available at our website: www.competitionpolicy.ac.uk.

CCP Response to the House of Lords on the Internet: To Regulate or not to Regulate

We welcome the opportunity to give evidence to the House of Lords Select Committee on Communications on several of the issues that have been identified as crucial to considering how Internet regulation may be improved. In our response we briefly address questions 1, 2, 5, 7, and 9 in the call for evidence and are available for further discussion on these topics.

1. Question 1: Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

1.1 Regulating the Internet as a whole is a very complex task that is unlikely to be efficient. A preferred approach would be to break down this very broad question by types of online services or categories thereof. Some services, such as social media platforms, seem to lend themselves better to co-regulation. For example, for platforms for sharing video content the way has been paved by the soon to be adopted revision to the Audiovisual Media Services Directive[578]. Though

[578] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (Text with EEA relevance) OJ L 95, 15.4.2010, p. 1–24; Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain

the UK might want to depart from this Directive in a post-Brexit world (should it be allowed to do so), the model of encouraging self- and co-regulation for the protection of minors and other consumers could still be followed. Where intervention by the regulator is necessary, we suggest a targeted approach aimed at specific types of services.

1.2 For the most part effective implementation and independent monitoring of existing laws governing a range of issues such as data protection, intellectual property rights, competition, or defamation, together with minimal additional internet specific legislation could ensure better protection of the various interests at play than extensive legislation aimed at regulating the Internet. Emphasis should be placed on establishing healthy legal frameworks within which self- and co-regulation can take place.

1.3 While there is real danger that over-regulation of the online space could lead to undue restrictions on expression, the devolution of responsibility to industry also carries a risk if self- or co-regulatory mechanisms are not set up well. The state has an obligation to ensure that efforts to protect intellectual property rights, rights to dignity, security or privacy do not overly impinge on rights to expression and information or the right to assembly (virtually). Most models of self- and co-regulation in other industries do not involve large individual companies making the decisions that involve the balancing of these rights based with reference to their own terms of use or community guidelines and its interests in maintaining its user base and advertisers. They involve collectively determined standards or codes, public involvement or at least consultation, effective appeal mechanisms, and often, regulatory backstop and/or incentives. The British advertising industry, for example, came together to develop a Code of Advertising Practice that set common standards and Ofcom now backstops its enforcement in a co-regulatory arrangement. Press publishing across Europe is governed by self-regulatory systems that involve collectively set ethical codes, criteria and/or participation incentives set by the state, and often public involvement in the enforcement bodies[579].

2. Question 2: What should the legal liability of online platforms be for the content that they host?

2.1 Given the challenges brought by the advent of the Internet, several private mechanisms emerged to fill in the regulatory gaps. Currently, this is achieved through terms of use policies and voluntary cooperation between platforms with right-holders, police or other authorities (e.g. using regularly updated 'list' systems whereby a central list of blocked URLs or domain names are stored). A number of specific domestic instruments also exist such as the removal of terrorist material (i.e.

provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities COM/2016/0287 final - 2016/0151 (COD).

[579] Manuel, Micova, and Tambini, 'Reforming the PCC: lessons from abroad' (2012).

UK's terrorism Act 2006) or notice-and-takedown procedures for defamatory content and copyright infringements (deriving from the implementation of article 8(2) Information Society Directive)[580]. Platforms can also be shielded against liability for the upload of infringing materials by third parties until they are being notified, following which they must act 'expeditiously' to remove the infringing content (i.e. article 14 E-Commerce Directive)[581]. Therefore, the current situation and blocking measures rely primarily on contractual terms established by platforms.

2.2 Whilst most platforms act as mere conduit, some companies have voluntarily gone a step further and taken proactive steps to detect or identify and determine which third party uploaded content (i.e. dominant platforms) should be available. Nevertheless, most current platforms do not act as publishers. This should be noted before deciding to change the legal liability of platforms. Additionally, it seems more appropriate to distinguish the activities of platforms rather than trying to classify them wholly as mere conduit or publishers as a platform be doing the activities of both. We have serious concerns as to extending a monitoring obligation to all platforms (especially due to the tendency to remove more content) reduces the possibility for dissemination of user-generated content, limiting freedom of expression. There is a difference between platforms being the best placed to *identify* content and them being best placed to *act/assess* whether there is indeed an infringement and therefore, whether the content should be available on the Internet.[582]

2.3 The main pressing change necessary to the current liability rules is better transposition of international standards in UK law, such as some instruments adopted by the Council of Europe including the Protocol to the Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems and the Convention on Prevention of Terrorism which are yet to be ratified by the UK Government.

2.4 Any specific legal framework should define grounds and conditions upon which content is made unavailable (whether through filtering, blocking or taking down) to ensure that freedom of expression (and freedom of information) is preserved online. To safeguard these fundamental freedoms, the grounds for refusing access to content online should closely mirror the limitations to freedom of expression as enshrined in article 10(2) of the European Convention of Human Rights (ECHR), namely: the protection of national security, territorial integrity or public safety, the prevention of disorder or crime, the protection of health or morals, the protection of the reputation or rights of others, and the

[580] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, Official Journal L 167, 22/06/2001 P. 10 – 19.

[581] Jacques and al., 'Automated anti-piracy systems as copyright enforcement mechanism: a need to consider cultural diversity' (2018) 40(4) *European Intellectual Property Review* 218-229.

[582] Ibid.

prevention of the disclosure of information received in confidence. The balance struck between the competing interests at stake on the grounds for rendering online content unavailable should preferably not be left to the courts or to private entities (i.e. intermediaries) but should be enshrined in the law and implemented through effective self- and co-regulatory systems. There is currently no need to add grounds for limiting online expressions to the list enshrine in article 10(2) ECHR. Nevertheless, conditions should also be specifically defined to avoid creative judicial interpretation. Although, national sensitivities and cultural diversity should be preserved which may lead to different judicial outcomes.

3. Question 5: What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?
Question 7: In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

3.1 Two things are crucial in terms of the way platforms act to balance online safety and freedom of expression and information: transparency and appeal. Of course absolute transparency in the algorithms that sort content or execute filters is not possible, in the same way it is not possible or necessary to have complete transparency of the thoughts inside the heads of each member of a press council that is deciding whether an article is libellous or headline hate speech. Transparency goes hand in hand with effective appeals mechanisms. In the same way someone can appeal a decision by Ofcom or a press regulator based on an understanding of the broadcasting code or editors code that were supposed to be the basis for that decision.

3.2 Some platforms have introduced complex algorithms capable of monitoring content online as well as complaints mechanisms to challenge decisions made by said algorithm, but a lot remains to be done to make the process transparent and fair. Important questions remain: how do these private companies monitor content and what ‘flags’ trigger action. When responding to notifications from users, what criteria are used to determine whether the contents should be removed? Aggregate data on removals of content for copyright, hate speech, security or other concerns, and on de-listing for data protection reasons is lacking making it difficult to monitor the balancing of fundamental rights.

3.3 Platforms could do more to ensure the protection of freedom of expression online (e.g. if algorithms can detect copyright infringements, these same algorithms should also be able to detect the possible application of copyright exceptions which could then be confirmed by human oversight), but the current incentives favour removal of content.[583] Content is increasingly being removed as pressure mounts for platforms to combat hate speech or fake news. Since the Facebook, YouTube, Twitter, and Microsoft signed up to the Code of Conduct on countering illegal online hate speech, for example, removals of content reports as hate speech increased from 28% to 70%.[584] Therefore, without jeopardising the application of safe harbour provisions, the attention of authorities should re-focus on also providing more incentives for platforms to respect human rights rather than just on controlling expression.

3.4 Effective appeal mechanisms are crucial to well functioning self- and co-regulatory systems and a lot more could be done regarding counter-notification or appeal mechanisms for platforms. Currently, such mechanisms as operated by Google on YouTube do not require human oversight and rely on the user to be able to articulate why the content is lawful within a certain number of limited characters. This process should be simplified for the user by removing any statement deterring them from challenging the decision applied by an algorithm, providing further explanations to users to help them in formulating a counter notifications or appeals, and verifying whether they should pursue the upload of particular materials. Information on the criteria being used to instruct algorithms or otherwise evaluate content could be provided to help users understand how their content is being assessed, and platform response to counter-notification or appeals should be monitored and compared regularly to take down or blockage data.

4. Question 9: What effect will the United Kingdom leaving the European Union have on the regulation of the Internet?

4.1 Many directives and regulations (including the GDPR and the Open Internet Access Regulation) will cease to have effect in the UK after March 2019. As the UK government intends to implement all EU laws into national law before departure, the legal framework is likely to remain the same as in the EU territory for the time being. However, the UK will not benefit from the developing CJEU case law in this area. If there is a willingness to consult the CJEU jurisprudence after March 2019, there is no certainty that the UK will follow and endorse the developments of the CJEU.

4.2 Furthermore, leaving the Digital Single Market is likely to have a dramatic impact on the UK as it will have to comply with EU rules in order to trade without being able to influence these. Historically the UK’s influence on EU communications policy has been very high, with UK expertise and pressure being particularly influential in the liberalization of telecommunications and audiovisual markets, not least because of the research capacity and expertise in its regulators. Leaving

[583] Jacques and al., ‘An empirical study of the use of automated anti-piracy systems and their consequences for cultural diversity’ (2018) *SCRIPTed* (forthcoming).

[584] European Commission, Results of the 3rd monitoring exercise of the implementation of the Code of Conduct January 2018 http://ec.europa.eu/newsroom/just/document.cfm?doc_id=49286.

the EU, the UK will lose its leading role in shaping one of the largest markets and in policy innovation that is often copied in other markets around the world.

11 May 2018

Centre for International Governance Innovation – written evidence (IRN0014)

Abstract: This submission by the Canadian-based, Centre for International Governance Innovation, which is an independent and non-partisan think tank, encourages the government of the United Kingdom to continue with its light-handed approach to regulating the Internet's infrastructure even as it, along with other Western governments, confronts new challenges in the online platform space. However, as with the infrastructure and architecture of the Internet itself, great care must be exercised to avoid curtailing the benefits offered by online platforms, while providing incentives and, if necessary, controls to avoid problems as they become evident. The elements of this approach include *inter alia* an "observatory" to monitor and publicly report on what actions are taken by the platforms and how effectively they are dealing with the public's (and the government's) concerns; a co-regulatory approach, involving the public sector with the companies to find solutions that the two parties agree will address the identified problems; and a multi-stakeholder approach to governance that goes beyond consultation in developing new legislation and regulation.

INTRODUCTION

1. The Centre for International Governance Innovation (CIGI) is a Canadian-based, independent, non-partisan think tank with an objective and uniquely global perspective. Our research, opinions and public voice make a difference in today's world by bringing clarity and innovative thinking to global policy making. By working across disciplines and in partnership with the best peers and experts, we are the benchmark for influential research and trusted analysis. Our research programs focus on governance of the global economy, global security and politics, and international law in collaboration with a range of strategic partners, and support from the Government of Canada, the Government of Ontario, as well as founder Jim Balsillie.

2. One of our Research Areas is Internet Governance & Jurisdiction. In collaboration with the Royal Institute of International Affairs, CIGI launched the Global Commission on Internet Governance, whose *One Internet* report makes practical recommendations for the international community to ensure that the future of the Internet remains open, secure, trustworthy and inclusive. The recommendations continue to gain traction on cybersecurity, multi-stakeholder governance and accessibility. CIGI is also conducting work on international economic law and intellectual property law related to Internet commerce. In March, 2018, CIGI and the Global Digital Policy Incubator at Stanford University in co-operation with the Department of Canadian Heritage convened an international expert working meeting to engage on the topic "Governance Innovation for a Connected World: Protecting Free Expression, Diversity & Civic Engagement in the Global Digital Ecosystem." These activities inform the following submission.

3. This submission draws on CIGI’s extensive work with partners and related research and is offered in response to the Call for Evidence by the House of Lords Select Committee on Communication inquiry, “The Internet: to regulate or not to regulate?” Specific recommendations in the text below have been highlighted in italics.

THE ESSENTIALS

4. The Internet is a vital engine of economic growth and innovation in all aspects of our societies. It is increasingly vital to our social life, through the online platforms that mediate individuals’ use of the Internet. In considering the question of whether or not to regulate, it is important to distinguish between the Internet and the online platforms. The Internet itself is an enabling infrastructure whose development has benefitted from governments having taken a light-handed approach to regulation in most cases, preferring instead to deal with specific problems as they become evident as, for example, in seeking to protect network neutrality and to regulate certain aspects of electronic commerce.

5. We encourage the government of the United Kingdom to continue its light-handed approach to regulating the Internet’s infrastructure, as they have in the past.

6. Innovative online platforms such as content delivery services and social media have extended the reach of the Internet to a vast majority of the population of the Western world and billions more in the developing world. Based on new business models funded by advertising, these platforms provide services and opportunities that could not have been imagined previously. Those have proven to be a boon to society, encouraging freedom of expression, expanding opportunities for political engagement, and enabling extraordinary access to a wide diversity of content, points of view and languages. However, of late it has become clear that the ubiquity of these platforms, and their business models based on the accumulation, manipulation and use of extraordinary volumes of data have also been abused by the platforms, by their customers and by their users.

7. There is now a high level of public awareness that such abuse poses a threat to individuals’ personal data and privacy, to democratic institutions and to the cohesion of society itself. Furthermore, the market dominance of the leading platforms is itself becoming a threat. Their near monopolies in their sectors put in doubt the sustainability of the professional press and that of the creators and distributors of diverse local and specialized content, cultural expression and languages. The public and the press are demanding action. For example, Canadian Heritage Minister Mélanie Joly has said that Internet platforms have “not basically accepted they have a clear responsibility” to the countries they operate in, including promoting and funding cultural content, but also shaping public debate and discussion. [1] Many of the platforms are scrambling to reduce the risks and governments around the world are trying to find ways to respond effectively.

8. Many of the international experts at the working meeting convened by GDPi and CIGI believe that recent events suggest that regulation in some form is now inevitable, but they advocated a "least force necessary" approach.

9. Recognizing that there are problems, great care must be exercised to avoid curtailing the benefits offered by online platforms, while providing incentives and, if necessary, controls to avoid problems as they become evident. This submission is intended to review the options for action that CIGI believes are available. We believe it is important to retain the greatest possible opportunity for innovation, for free expression, and for cultural diversity on the Internet, while and seeking to forestall the forces that seek to do harm under the guise of exercising those rights.

10. CIGI's work with the Global Commission on Internet Governance (GCIG) and more recently on how best to protect free expression, diversity & civic engagement in the global digital ecosystem points to several reasons to be cautious about trusting to traditional national legislative or regulatory processes to address problems such as those now raising concerns. There are several reasons for this caution.

11. The Internet and the online platforms that mediate individuals' use of the Internet are characterized by continuous, often rapid and occasionally disruptive change. Those characteristics are likely to remain a constant. Democratic governments are unlikely to be able to keep up by means of their intentionally slow and deliberative mechanisms. Nor are they usually able to monitor and react quickly to changes in online services or market structures.

12. Any response that hopes for success should be light-handed, flexible, broadly applicable and based on widely-agreed social consensus. To be credible their requirements and results also need to be transparent. The GCIG recommended taking this approach in its report, launched at the OECD Ministerial Meeting in 2016 [2].

13. These goals are difficult to achieve through legislation or regulation. For that reason, to the extent possible, Her Majesty's Government should consider taking a graduated approach when it is considering the question posed by this Inquiry: "The Internet: to regulate or not to regulate?" One series of steps in a graduated approach is suggested in the following.

14. A graduated approach might begin by urging self-regulation by the platforms themselves. Two motivations could encourage success. The platforms may recognize the problems and seek to correct them to the benefit of their customers and users, or the platforms may want to use self-regulation to avoid more forceful government action. Several of the major online platforms are already taking action, although it is far from clear that they are taking a sufficiently thorough and well-thought-out approach to satisfy the need.

15. A second step could be to put in place an “observatory” to monitor and publicly report on what actions are taken by the platforms and how effectively they are dealing with the public’s (and the government’s) concerns. This function need not be performed by a government body; it could be undertaken by an independent civil society or academic entity either voluntarily or with a governmental mandate and support. Online platforms could be required to fund this work, perhaps through a dedicated levy. Sometimes called a “name and shame” approach, the independence, transparency and reputation of the overseeing body serves as a greater incentive to platforms addressing their problems in a thorough manner.

16. A third step could be for the government to require a co-regulatory approach, involving the public sector with the companies to find solutions that the two parties agree will address the identified problems and also satisfy the public interest concerns identified by governments. A co-regulatory solution could be implemented by mutual agreement or it could be required by governments. Co-regulatory approaches typically will include requirements for transparent reporting on the steps taken and their results. An auditing function may also be imposed, to assure the public that the reports and results are accurate. The audit could be done either by government or by an independent body, as in the previous example.

17. A fourth step could be to initiate a multistakeholder approach to addressing the problems. Multistakeholder approaches go beyond consultation, in that they are aimed at achieving a shared, consensus solution to a well-defined problem. A process to deal with a problem must show that it is broadly inclusive and committed to transparency help so as to establish the basis of its legitimacy. Participants must come in agreed about the goal of the process and committed to finding a solution. To be successful a lot of preparatory work is required, linguistic and cultural barriers will need to be addressed, and resources must be available to pay for a range of items, including attendance at meetings and time away from paid work. Often the work has to be done without having a firm guarantee that the results will be enforceable. Yet, when the alternative is that nothing at all will happen, there is little to be lost in trying to get to a solution through a multistakeholder approach. Another advantage is that it is much easier to fix or tweak multistakeholder outcomes than laws. A fine balance has to be reached to get sufficient confidence in governments’ willing to stand behind a solution to justify the cost, effort and risk of committing to a complex and difficult process.

18. The ultimate step in a graduated approach would be the imposition of government regulation or legislation but, for the reasons outlined previously, this approach should only be undertaken as a last resort. That said, both the European Union and Germany have chosen to legislate and regulate in this area. As the Select Committee will be aware, both are learning that implementation is fraught with unexpected difficulties.

19. A final challenge faces any national government that attempts to impose legislated or regulatory control over online platforms – that of jurisdiction. As Michael Chertoff and Paul Rosenzweig wrote for the GCIG, "At the heart of this problem is the question of which nation and which nation's laws are able to control the disposition of a matter. It reflects both a narrow power — that of a court to adjudicate a case and issue an order — and a broader concept of defining the territorial and lawful bounds within which a court, agency or government may properly exercise its power and authority."[3] The global scope of the Internet makes online platforms accessible in almost every part of the world; thus they may face different requirements from a range of countries and cultures. Governments' attempts to impose different requirements could easily lead to fragmented services or, in the worst case, a fragmented Internet. Already there are examples that demonstrate that this is not an unlikely outcome, such as the uneven application of the European "right to be forgotten," or the Canadian Supreme Court's Equustek ruling which has been overruled by a United States District Court in California [4]. Clearly the platforms, their users and society as a whole will be the losers if that is the outcome of governments' competing or inconsistent regulations.

20. *The best solution to the current spate of problems concerning governments and the public is to seek an internationally agreed approach, perhaps starting by seeking agreement among stakeholders in liberal democratic states That is the recommendation of the GCIG, in its call for a Social Contract for Digital Privacy and Security. [5] Drawing on the inspiration of that call CIGI recommends that this vital internationally agreed approach be built on a shared commitment by all stakeholders in developed and less developed countries to take concrete action in their own field to build trust and confidence in the Internet and the online platforms. A commitment to the concept of collaborative security and to privacy must replace lengthy and over-politicized negotiations.*

21. Taking these comments and recommendations as a framework, CIGI offers the following responses to the specific questions posed by the Select Committee where we believe our research and collaborations can benefit the Inquiry.

RESPONSES TO SPECIFIC QUESTIONS

QUESTION 1: Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

22. *See Paragraphs 9 and 12 above.*

QUESTION 2: What should the legal liability of online platforms be for the content that they host?

23. *It would be difficult if not impossible to hold online platforms responsible for the content they host without seriously compromising the value of their services. The best approach would be to hold the platforms liable for content they host once a problem is drawn to their attention, whether by users or by governments.*

QUESTION 3: How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

24. *A multistakeholder approach would be well suited to developing guidelines for online platforms to use when moderating content, taking into account the differences among national value sets. The guidelines could include appropriate appeal processes. An independent oversight group should oversee implementation of the guidelines. Please see Paragraphs 15 and 16 above.*

QUESTION 4: What role should users play in establishing and maintaining online community standards for content and behaviour?

25. *Users should play a pivotal role as part of a multistakeholder process, including oversight by an independent group. Please see Paragraph 16 above.*

QUESTION 5: What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

Online platforms should be required to meet or exceed community standards developed to address concerns in these areas, as recommended in paragraphs 15 and 24 above. Protecting the rights of freedom of expression and freedom of information should be understood to include explicitly the responsibility to ensure *the availability and discoverability of content reflecting regional and local cultural diversity and language.*

QUESTION 6: What information should online platforms provide to users about the use of their personal data?

26. *The platforms should be forthcoming and transparent in providing information to users about the use to which their personal data is being put. This information should be included in their terms of service. The explanation should be easy for users to locate and expressed in plain English at the time of signing up to use the platform. Users should be reminded of this information annually, and in addition should be notified of any changes before they take effect. Users should have the ability to unsubscribe from the platform if they disagree with the use of their personal data.*

QUESTION 7: In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

27. *The online platforms should inform users about their business practices, including their use of algorithms in the same ways recommended with regard to the use of personal data (paragraph 26). They should not be required to reveal proprietary information, but should provide sufficient information for their users to make an informed decision about whether they wish to continue their use of the online platform or not. By analogy, a soft drink manufacturer should be able to assure the public of the*

safety of their product without having to reveal their product's proprietary formula.

QUESTION 8: What is the impact of the dominance of a small number of online platforms in certain online markets?

28. In most jurisdictions, measures are in place to control against monopolistic behaviour in a market segment. Consideration should be given to putting in place similar disincentives in the online world. Market dominance is undesirable because it can make it very difficult for new entrants (or even new services) to gain a toehold as competitors. It can therefore discourage innovation. It also can work against the availability and discoverability of content reflecting regional and local cultural diversity and language.

QUESTION 9: What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

29. *The departure of the United Kingdom from the European Union brings will require an extensive review of its regulatory framework in all areas including the many areas where the EU has undertaken a unique approach toward regulation of the Internet. The necessity to replace the EU approach presents an opportunity for the United Kingdom to take a new approach by working with all stakeholders to develop a new social compact for the governance of the Internet, as recommended by the Global Commission on Internet Governance. Success in this endeavour would make the UK a global leader in an area of ever greater global importance.*

REFERENCES:

[1] https://www.thestar.com/news/canada/2018/03/14/internet-giants-should-support-local-news-culture-melanie-joly-says.html

[2] https://www.cigionline.org/publications/one-internet

[3] https://www.cigionline.org/publications/primer-globally-harmonizing-internet-jurisdiction-and-regulations

[4] https://www.thestar.com/business/2017/11/03/canadas-top-court-overstepped-cant-enforce-google-to-delist-search-results-in-us-judge-rules.html

[5] https://www.cigionline.org/publications/toward-social-compact-digital-privacy-and-security

8 May 2018

Centre for Policy Studies, Centre for the Analysis of Social Media at Demos and Institute for Public Policy Research – oral evidence (QQ 52-57)

Tuesday 22 May 2018

Watch the meeting

Members present: Lord Gilbert of Panteg (Chairman), Lord Allen of Kensington; Baroness Bonham-Carter of Yarnbury; The Lord Bishop of Chelmsford; Lord Goodlad; Lord Gordon of Strathblane; Baroness Kidron; Baroness McIntosh of Hudnall; Baroness Quin.

Evidence Session No. 7 Heard in Public Questions 52 - 57

Examination of witnesses

Robert Colvile, Director, Centre for Policy Studies; Jamie Bartlett, Director, Centre for the Analysis of Social Media at Demos; Laurie Laybourn-Langton, Senior Research Fellow, Institute for Public Policy Research.

Q52 **The Chairman:** Can I welcome our second set of witnesses to our evidence session this afternoon on our inquiry into regulation of the internet? Our witnesses are from three prominent think tanks who are working in this area: the Centre for Policy Studies, the IPPR and Demos. I thank the three witnesses for being here. The session will be broadcast online and a transcript taken. Can I ask the witnesses to briefly introduce themselves, tell us a bit about their organisations and perhaps start by giving their initial impressions on the issue of regulation from an economic perspective, the dangers of poor regulation, the impact that it can have on start-ups and innovation in the sector and the likelihood of big tech companies locating in the UK if we create the wrong kind of regulatory environment?

Robert Colvile: I am the director of the Centre for Policy Studies. Before that I was a journalist at the *Telegraph* for 10 years where one of my main areas was technology. I wrote a book called *The Great Acceleration*, about how the internet is speeding up the pace of life, including politics and the media. I then migrated into think tank-ery. Our organisation is a free-market think tank devoted to policies that promote opportunity, enterprise, aspiration and ownership—and, obviously, the internet is now threaded through the economy completely. In terms of regulation, the starting point for Britain should be that it is in a good place. It dominates Europe in terms of tech investment. We have a higher percentage of tech jobs in the UK than most other countries.

There are issues around the fact that the UK cannot grow its own Facebook and Google. I have written about this in the *Financial Times* and elsewhere. If the starting point, as with a doctor, is to do no harm, that is something that definitely needs to be borne in mind. There are tremendous issues and challenges thrown up by the internet but one of the dangers is regulating for the internet as a thing rather than thinking about it as a whole host of areas and activities which are deeply entwined between online and off—similarly, regulating for Facebook or Google and accidentally catching up with the rest of the economy in the process.

One of the things that I want the Centre for Policy Studies to get into under my directorship is the issue of monopoly policy because everyone recognises that we are in a situation now where the traditional template does not apply. The idea is if Airbnb were to get 80% or 90% of the market, but was still driving down prices for overnight stays, is there consumer harm and what can you do about it? What is the benefit of the traditional template of that? It does not work. I believe that is a fascinating area that we will have to explore over the next few years.

Jamie Bartlett: About five years ago I set up the Centre for the Analysis of Social Media—CASM—at Demos with the idea of trying to take techniques of machine learning that were being applied in the private sector and work out how to use it in academia and public policy research. We partnered with machine learning specialists at the University of Sussex and developed software, and methodologies and techniques for using those technologies in research work. I am the author of a book that is rather scarily titled, *The People Vs Tech: How the Internet is Killing Democracy (and how We Save It),* though the "how we save it" is in brackets, so it is almost an afterthought, unfortunately. I am especially interested in the ways in which digital technology is, in some senses, incompatible with modern representative democracies and how economic change driven by the internet will wear away at the fabric of the middle class, for example.

In respect of the question, even though my book would suggest that we do need to regulate more, I am especially worried about the risk of bad regulation here because the internet will change rather a lot in the next decade or so. It is changing very quickly already. There is a great emergence of censorship-resistant technologies which will make the way we understand who is responsible for content potentially change quite dramatically, and it will be very easy to pass very bad laws about how the internet works now, not thinking about how it might work in future. One of the great risks I see driving this is the great deal of political consternation about the role the internet is playing in politics at the moment. Some of that is driven by the way traditional news outlets are frustrated by their loss of advertising revenue to the big tech firms, which is causing some remarkable headlines that are not particularly helpful.

The final point about this is that I consider we are in a race with countries such as China over artificial intelligence and it is quite important that we win that race. China does not worry so much about user privacy and data protection and is investing a fortune in this. We have to find a way of regulating various aspects of the internet, as Rob said, not all the same, such that people still feel that it is democratically accountable in some way and they have some control over it, but that we stay ahead of countries such as China in the race for AI, and that is a very, very difficult thing to do.

Laurie Laybourn-Langton: I am a senior research fellow at the Institute for Public Policy Research where I work on the IPPR's commission on economic justice, our flagship programme, which is creating an economic platform for post-Brexit Britain, of which the internet and, by extension, platform companies are key parts. I have worked in economic policy for around five years, prior to which I worked in digital campaigning looking at how to translate digital tools for social action. Our main focus at IPPR when it comes to regulation of digital and the internet is platforms—those intermediaries of social and economic activity.

Our main point here is they have disrupted socioeconomic relations and the way we do things in the economy and society more than many other inventions in recent history and, arguably, as time goes on, more than at any point in the last few hundred years. Therefore, an appropriate response to that disruption is key and, we believe, ranks up there with the major challenges of our time, including the environmental challenge, pervasive inequality and many of the others that we often hear about.

On the regulatory challenge, the first point I would make is that we still need to work out what we are regulating, because of the extent to which these disruptions have worked into a variety of economic and social activities and some political activities as well. By its very nature, regulating becomes very hard because of the fast pace at which this disruption is occurring and permeating into markets that we do not necessarily associate with the first movers within this sector.

There will be an enormous cost in getting regulation wrong and there could be an enormous cost in getting it right, which goes to the heart of this problem around the power relations between the interests that are served by a lot of the first movers, the large companies having large interests increasingly in a number of sectors. As with many areas of regulation, we will probably not know whether and what kind of cost we have incurred until far into the future, which becomes particularly dangerous for a number of reasons, including around AI, which will increasingly undergird the infrastructure in which economic and social activity can occur in the future.

Q53 **Baroness Kidron:** One of the things that concerns us is that the conversation easily floats to content when the infrastructure itself, the design of services, the ways in which they work are the things that maybe we should be looking at more carefully. Could each of you say a bit about your thoughts or worries about some of the current norms of design, by which I mean filter bubbles, persuasive design technologies or the idea of machine learning, where the designer does not know what the outcome will be? Going to Mr Colvile's point of "do no harm", should we be designing them to do no harm and considering in advance what they may do? Could you speak to the design?

Robert Colvile: These sites are designed to succeed and, primarily and overwhelmingly, to foster user engagement, revenue, whatever the goal of the company is. They are ferociously well-equipped to do that by a process of constant iteration. David Cameron does march into Tesco and tell people not to put their chocolate oranges by the checkout, but he does not start telling them to shift the vegetable aisle 20 metres to the right and all sorts of other things. We need to be wary about doing things to interfere with the activities of online companies which we would not do offline because they happen to be on this thing called the internet.

Baroness Kidron: May I press you a bit and perhaps talk about the drug sector, big pharma, which does have bars that it must reach. No one tells them what to put with what, but they do have to think about the consequences of their design. I did not mean literally tell them how to design—but perhaps impact and consequences would have been a better way of putting it.

The Lord Bishop of Chelmsford: I believe sweets by the shopping tills is an extremely good example and not a trivial one at all, because I used it on a previous occasion. As a society, that is where we legitimately make decisions about design because we think there is a societal good to that.

Robert Colvile: The problem with any of these debates is that you get into a whole mess of areas. There is a conversation to be had about Facebook as a mechanism of constant engagement. The example I have used before is that if you "like" UKIP, which is a perfectly legitimate political party to like—people in this room might dislike it—it instantly shows you pages for the National Front and the BNP. It is constantly trying to intensify and radicalise your experience at the same time. I think and hope that they fixed that in the year since I found that, but it is a good example. You have questions of structure with things like Amazon—if you own the platform, should you be allowed to be a player on the platform? Ultimately, these companies succeed or fail by how well they serve their users; that is the metric. They are far more scared of doing stuff that would disappoint their users or lose their loyalty. That is the thing which drives them on. It is not a sinister plot to hypnotise our children into using Facebook. It is just that they are paranoid that they need to keep people happy and engaged.

The Chairman: It is about how good the markets audit.

Jamie Bartlett: Possibly. I am slightly more worried than Rob about addictive technology and design technology, but I agree that it is not a malicious plan. It is just that there is an impulse to work out how to make people spend more time on the site to collect more data. It is the underlying driving logic of how these platforms make their money. However, I do not believe that you should be in the business, therefore, of telling companies how to design platforms.

In this instance, I am talking of a self-regulatory, ethical body where companies sign up saying, "We are designing these platforms as something like a fair trade stamp whereby we are not designing them to be as addictive as possible. We are going to try to put in some default settings to make sure you are reminded that maybe you have been on this platform for an hour now and do you want a break?" There are some tech firms that do those things, such as Slax. Default settings is quite an interesting area where the default setting of whether your data is immediately shared or not has probably more influence and impact than any other small tweaking around the edges. There is scope for it to say, "Well, could you have your default setting at higher levels of privacy rather than at lower levels?" There are certain things that can be done.

It is interesting to talk about it now because advertisers talk about the "creep factor" in their work—an invisible line whereby it seems a bit weird and people do not like it very much, but understand it to exist. At the moment, it feels like we are on that line with addictive technology and a lot of tech firms have been quite explicit—including Mark Zuckerberg—that they feel they may have crossed that line and want to work on improving it. At this point, it is a good opportunity to work with the tech firms to try to do something about it.

You mentioned filter bubbles. It is an idea whereby like-minded people are clustered into silos of information and it radicalises them in one way or another, which is not entirely my experience, looking at the research base. We do have access to a lot of different views. When I am on the internet, sometimes I feel that I only ever see different views and they are all wrong and that is the problem. It is not about thinking that you are stuck in a filter bubble of like-minded people. There is a broader issue. Simply the way we communicate with each other online is very sharp, quick, and dramatic. We tend to overstate our enemies' or opponents' importance and significance, and we attribute to them all sorts of terrible motives that they probably do not have, and they do likewise to us. To me, that is a bigger problem than a filter bubble. Some people call that the backfire effect, which is the nature of internet communication. Essentially, it leads you to see a lot of other views but to disagree even more when you do see them.

Laurie Laybourn-Langton: The point I would make is that social, political and legal norms have been established over time in a number of areas of activity across the economy and society. Many of those standards are stronger for important types of activity, whether that be how we interact in democratic elections or in the provision of certain key economic goods, of which drugs are probably one—pharmaceuticals. I do not believe we have yet established those norms which are translated into regulation and policy for platforms and digital firms. A perfect example of this would be that today, the *Times* reported a story about how a video was leaked showing the development technologies that could lead to a better understanding of how we behave, to then pre-empt how they can manipulate our behaviour into the future.

If the Cabinet Office had a video like that presented to them and leaked, can we imagine the reaction that would rightly come about the potential for cracking down on people's liberties across the country and, indeed, the world? That shows a big disconjunction between the norms we have established in certain areas of society and those in this sector, particularly when we understand the activities that we take part in on Facebook and other platforms are increasingly akin to key essential services for the economy of gaining information, conversing with people, building political coalitions and those in the community. In establishing those norms and the regulations and policies that are attached to them, I completely agree with Jamie that the revenue model that sits behind a lot of these platforms is the key thing.

They create certain services, which are underpinned by algorithms that sift through data; they extract data and analyse that to gain insights, which create products which they can then sell. In the case of Facebook that is advertising. The impulse there is to extract more data to feed back to improve the analytics to further extract data and provide products that gain profit. There are three areas which we are looking at around policy in response to that. There are particular ones about how platforms develop the algorithms and the services that underpin their model. Do we need to introduce certain types of ethical behaviour when it comes to those that designed coding and algorithms, because we know that, famously, you often translate your own political or other biases into the programming that you take part in? Do we need professional qualifications that have similar ethical support, as well as standards that chartered accountancy has in this country and others?

Secondly, we then need to make sure that certain norms are translated into regulations. Another article on the front page of the *Times* today was about how some auto-response Google searches are beginning to potentially link those who are implicated in sexual assault cases with the victims because people have leaked those details on social media. Google is able to take some of those things down. There is a norm that we have in wider society about sharing that information—a legal one as well—that increasingly needs to be transferred to regulation.

A third area is increasing competition in some of these markets. I hope we will talk about that more. The one thought I would add at this point is that, in doing so, we need to break down this whole world of the internet and digital technology into certain functions instead of it lumping together.

Baroness Kidron: I was going to ask you about whether you should regulate but you have answered that. All the witnesses, of all kinds, who have come here all agree there is ethical component. What we are struggling to understand is where that sits. If you could very briefly say, in the conversation about “We should have ethics and norms”, and so on, who is “we”?

The Chairman: This is something we want to get to. We have been asking witnesses about the “who.” There is clarity about what the industry needs but not about whether there is regulation, law and who is responsible for bringing this together.

Baroness Kidron: Because they suggest they would like to be the author of the ethics. That is complicated in itself. Where does that duty sit, the creation of an ethics context? Anybody? Any brave man?

Jamie Bartlett: As I have said, when it comes to addictive tech in particular, it is a question of self-regulation. It should be encouraged and welcomed by government, but, in the end, we should at least first try with self-regulation.

The Chairman: Can you help us with the steps to encouraging the industry? You talk to the industry and have an understanding of where they are coming from on this and, from your answer, you are optimistic that they understand it and want to get to the same place. What steps should be taken by government to make that happen with the industry?

Jamie Bartlett: I do not feel well enough qualified to answer that. You are probably more experienced with the ways in which governments have been able to encourage good self-regulation. In the alcohol industry, they bring a large body of players together, talk about the different ways in which they probably should try to self-regulate better and if they want to set up a body, the government will be there to support it and there is the threat of regulation if they do not do it. That seems to be the way that it usually works.

Laurie Laybourn-Langton: I will make three points on this question of who is one of the most important ones. First, this is enormously complex. We are talking about platforms that engage in activities that span from payment services all the way through to providing a way to have a political argument, build a coalition, take a petition to Parliament. The regulatory response is not going to catch all that in one go. We should break it down into the particular activities under the purview of these services.

Secondly, within that, there needs to be future focus. Your regulatory response to whether you can, without impunity, place what we would probably define as hate speech in a public forum out there—the regulation or any approach we have will be vastly different from potential regulation to stop Google, for example, from developing technologies that are able to nudge or manipulate us in a way that we have not yet fully understood.

Thirdly, a kind of direct answer to the question of "who", I would say, is: not a small subsection of the leadership of the firms who provide these services, necessarily. A more general version of that is that, among the key regulatory challenges, this should be undertaken according to democratic principles, in the same way that we have provided regulation in other key areas of society and the economy through a democratic mechanism—Parliament and the people who represent us—as opposed to those whose revenue model dictates that they should focus narrowly on products they think could revolutionise the world.

Lord Allen of Kensington: Would it be helpful or not to fund an independent body or to fund what could be done in this area?

Laurie Laybourn-Langton: Taxation has to be part of the toolkit, but, again, it depends upon which particular activity you are seeking to regulate. For example, you could tax more heavily the provider of an on-demand taxi hire service in a city if it does not list vehicles that are electric.

Robert Colvile: It is generally accepted that, at least in terms of the early years, the tech firms did not take responsibility for what was happening on the platforms. Mark Zuckerberg stood up again and again and said, "We are a platform, not a publisher", which coincidentally and helpfully means they do not have to spend lots of money hiring people to police content. No one can police the internet, but it is probably fair to say they were not trying very hard. That has changed now as the backlash has grown. They are investing far more in that kind of thing. The Conservative manifesto in 2017 was littered with commitments to impose better behaviour, to push the internet companies to behave properly and make sure that what was illegal offline was illegal online, and to prevent hate speech. I have a printout here. It was quite a lot of stuff. In many ways that manifesto has been inevitable.

I do worry that there may be some slight rule of unintended consequences to some of this. We have seen it with the GDPR, which I imagine we may get on to later. The big companies can afford the lawyers and the squadrons of people policing all the comments and writing the algorithms to hunt down Islamist videos and all the rest of it. As with quite a lot of regulation in quite a lot of sectors, in many ways what that does is deepen the moat around them and make it harder for people to compete with them. In certain cases—Jamie has written about this—it may drive the more unsavoury behaviours into a wild west, which may be impossible for the authorities to see, let alone regulate, especially with advances in crypto-technologies.

Baroness Quin: What are your feelings about whether there is a need to strengthen the consumer voice in this process and, if so, how to do something about it? What are your feelings about the role of education? It seems to me that a lot of us—I certainly include myself—use the internet for convenience but, in accepting cookies and goodness knows what, do not understand a lot of the time how much information about ourselves is being shared in a way that perhaps, as individuals, makes us feel uncomfortable. I certainly feel in that position myself now, having done so much online and suddenly realising that in accepting all these cookies and so on, all kinds of information is out there. Related to that, Jamie mentioned having some kind of default setting that gave a higher privacy standard. Could that be done by self-regulation, or ought it to be legislated for? Is it covered in existing legislation? I do not know.

The Chairman: Shall we start with education and citizen empowerment, Mr Bartlett?

Mr Bartlett: I will clarify something. When I was talking about self-regulation, I was referring specifically to the point of addictive tech and design. As you said, Laurie, it depends what problem you are trying to deal with. On user education, when I first set up CASM five years ago, we wrote a big report talking about the value of and need for better education on digital media literacy in particular, i.e., the ability to distinguish between truth and falsehood online. Every single report that any think tank ever writes ends up saying, "We need more education". The curriculum will be 150 hours long a week to include all the content we need.

Of course, I think that but I accept that will never be enough. It is an easy one to default to. There are certainly ways in which we can improve the way media literacy is taught. Google's algorithms are not as powerful as our own cognitive biases in terms of how we filter information. If we have media literacy classes improved, it needs to include cognitive psychology rather than just technology. There are certainly things we can do but it will never be enough.

Interestingly, I do not think any company has done more for the cause of user privacy than Cambridge Analytica. Everyone is now talking about it and thinking about it in a way they were not before. The way that the population tends to learn about these things is through things going badly wrong and us taking the opportunity to think about it and have a bigger public debate about it. There is a certain way in which public education moves independently of schools. That is very healthy and has been quite a good thing over the last couple of weeks. Honestly, when it comes to legislation on default settings, it is something I am not sure about. To be honest, I cannot decide. GDPR has some things on that, but it is a difficult one.

Mr Colvile: On education, I would echo what Jamie says. Obviously, we need to increase digital literacy, but that is much harder than writing reports saying we need to increase digital literacy. There is some encouraging evidence that young people are more privacy savvy than their elders, and are using Facebook in ways which preserve their privacy and migrating to other networks because they do not want their parents finding out, which is perhaps the most important form of privacy when you are that age. Regarding consumer power, consumers have voted in overwhelming numbers. Some 70% of the UK now uses Facebook.

Mr Bartlett: A high proportion of people also say they do not trust the company or they do not like the company.

Mr Colvile: I agree with that, but if you look at the results that came out after it had this amazing storm of bad publicity, guess what? No one is giving it up. Consumers like these services, which is part of the problem because it is hard to regulate something when everyone is using it and is quite happy with it. The person who stands for election on a manifesto saying, "We will break up Google's monopoly", will be horrendously unpopular.

The privacy by default issue is interesting but there is a tension here between privacy and progress. I am not talking about Facebook in particular. Things such as NHS data in particular—doing the cool stuff with AI requires access to very large data pools. As Laurie has pointed out, we may not want them doing some of the creepy cool stuff. The value to Google is not that I am searching for a Chinese meal at this current moment or even that I tend to like Chinese meals; it is that people of my age, weight and location tend to like Chinese food and in 20 years' time we will all die of heart attacks. That is the real goal that you are trying to reach in quite a lot of this.

The more privacy rules you erect, the more—this is not saying we should not give people as strong privacy as they want, but we need to recognise that the model relies on data being shared and analysed and that does good things for the rest of us. If you said to people, "You can have higher privacy settings on Facebook but you have to pay £10 a month to use it", that is a very different proposition from, "You get the privacy, but they don't get the data".

The Chairman: I am sorry. We need to move on. Mr Laybourn-Langton.

Mr Laybourn-Langton: Education: there is lots of low-hanging fruit there, particularly regarding those who did not necessarily grow up with these technologies. The consumer point that Robert made is important and goes to the heart of the regulatory problem here. The original rules of regulation or ways of looking at the world are around price and impacts upon consumers. At the first instance, this is all very pleasing for consumers and this is where you probably have limits to education.

Can I make another comparison between a service and people's ideas of liberty and government? If, one year ago—five, 10, 20, 50 years ago—you suggested that you would voluntarily put a device on your person that mapped where you went all the time and you openly allowed it to infer, based upon that data, where you lived, where you shopped, where you worked, where you did all sorts of other activities, the uproar would have been extraordinary. Because we have a lot of pleasing elements for consumers, it means that that disjoint exists. That is a serious issue that we all have to deal with. That is not about regulation; it is about how we interpret society.

That regulatory response needs to be properly resourced so that experimentation can occur. It can be asked whether we should have default settings and the like. We should experiment; that is the very nature of this sector. It is very fast-moving, it is experimenting all the time, and there is potentially room for regulators in certain small areas to experiment around certain products even in a safe atmosphere. I know this is increasingly happening in the financial services industry where regulators are looking at how to experiment in what they call sandpits, where they can look at certain products and what that means.

Q54 **Lord Allen of Kensington:** To what extent should online platforms be liable for the content that they host? Specifically, should the safe harbour provisions of the e-commerce directive be removed?

The Chairman: You have already addressed some aspects of this, so brief answers would be fine.

Mr Bartlett: No, they should not. As with publishers, it would more or less destroy most of the social media platforms if they were liable for all the content that was hosted there. The task is to make them as quick as possible at removing content that is identified as illegal, twinned with some self-regulation. The German model is a reasonably good one: high fines where they do not remove content within 24 hours if they have been told there is illegal content there. They face fines of up to €50 million. There is backstop legislation that encourages them to be much quicker and more responsible in removing content when it is alerted to them.

Advertising might be slightly different. Given that they are paid to put that content up there—this is obviously the Martin Lewis case that is going on at the moment—there is a case that that might be slightly different and that they should be liable for the content that they advertise on. One of the reasons why it is quite dangerous to go down the line that they should be liable for all of it and we remove the e-commerce directive safe harbour provision is that the internet is changing. In the next 10 years there will be a lot more decentralised blockchain-based platforms where it will be very hard for the companies that run those platforms to be able to remove content at all because they will be hosted on distributed immutable ledgers, at which point there is no technological capability that would allow them to even take it down. Therefore, for them to be responsible for that would be an extremely difficult case to make.

The Chairman: Mr Laybourn-Langton, I am particularly interested to know, do you recognise that distinction between content and advertising content?

Mr Laybourn-Langton: Yes. An equivalent would be that you could stand outside Parliament here and you could say something in that forum, or imagine a situation where Parliament Square would earn money from your ability to say those things. Those are clearly distinct areas, so I would agree with that. What Jamie is saying is absolutely right, and with new blockchain-based technologies it will become harder and harder to do this as time goes on. If you were to set that principle now, pressure would need to be applied to ensure they were moderating that content as quickly as possible.

On the question of safe harbour, we do not have a particular view on that but note that the gap between the value that YouTube is getting out of those who have created certain content and the money they receive in return is obviously opening widely. We do not have a specific view on that.

Mr Colvile: This will be shocking: the director of the Centre for Policy Studies will praise a European regulation. The safe harbour provisions work pretty well. There is an obligation to act expeditiously to remove or disable access to the information. I agree with Jamie that removing it would be disastrous. It is the internet equivalent of a limited company. It is what gives you the protection to start up a company and not be liable. Having edited a newspaper website, I know that it would have been apocalyptic if we had been liable for everything people said in the comments section. There is also an economic point: if you want a single way to guarantee that no one will ever create a new technology business in this country, removing the safe harbour provision would probably be one of the top three things you could do to make this a hostile place for people to invest.

Lord Allen of Kensington: Blockchain or whatever comes after it is in itself pretty scary, because we are trying to legislate and regulate for something that has not even been thought of. Do you have any comments or thoughts on how we can try to move ahead? Frankly, legislation is always too slow in these areas and your comments on that struck home to me.

Mr Bartlett: I am struggling greatly with this. In my first book, *The Dark Net*, I looked quite a lot at blockchain technologies. That was in 2014 and I could not see an easy way to deal with this. I do not think there is one. There is some enabling legislation or regulations that could be passed about how initial coin offerings should be managed and run. I know a lot of blockchain companies want guidance from government about how they should deal with some of these problems and there is none out there at the moment. For me, the first step is to create some kind of enabling environment for these companies to operate. Most want to work within the law; they do not know what the law is because there is not any law for it.

Honestly, when it comes to the issue of censorship in particular I do not think we have an answer. It is genuinely possible that we are entering into a world in which censorship of the internet becomes close to impossible. Governments will inevitably pass draconian measures to punish the people who posted that content because deterrence will become the most effective means of making sure bad material is not posted. That is the direction of travel I imagine it will go down, which worries me.

Q55 **Lord Gordon of Strathblane:** Moving on to competition law and its adequacy for the current environment, I was taken, Mr Colvile, by a remark you made in your opening comments about where the public interest lies if Airbnb achieves 90% of the market but is still driving down prices while maintaining standards. It is an interesting point because it seems to me that monopoly is almost built into the digital environment. It is unthinkable that Google's market share will drop from 94% to 40%. Things do not work that way. How do we cope with it? Is regulation the answer to ensure that the monopolies are acting in the public interest?

Robert Colvile: If I was locked in a room for three months and told, "Go away and solve one public policy issue", this is what I would devote myself to. It is utterly fascinating and vitally important. Amazon is the best possible example of this. To some extent, Amazon's stratospheric share price is predicated on eventual monopoly. People are effectively making a bet that it will grow and grow and swallow more and more markets. In the process it will deliver enormous value to consumers, who absolutely love it. It will put the squeeze on quite a lot of producers, as Walmart and Tesco did in their day. It is almost more powerful. In the old days, if you were a retailer you could get space on the top shelf in the supermarket. Now, no one scrolls on to the second page. The result that comes up at the top of Amazon is almost certainly the thing that you buy. Likewise, the result that Alexa gives you when you say, "Alexa, order me some milk" is the thing that you buy. If Amazon has its own brand of milk, at that point that is an incredibly powerful proposition. Yet, it is delivering benefits. It is a tricky thing to untangle.

Ben Thompson writes *Stratechery*. It is extremely good. One of his suggestions, for example, is that no one with a dominant position on one platform should be allowed to buy another platform. Facebook should not have been allowed to buy Instagram and WhatsApp because that has entrenched its position. We need to start thinking about indirect monopoly. Even when the domination of the home market is not anti-competitive, it generates enormous profits that can be used to buy other companies, invest in other areas and expand. Google is doing self-driving cars and AI, which is all funded by the core advertising monopoly. The problem we have is not that these companies have done anything wrong. It is that they have done everything right and they are in markets which are structured to deliver outsize rewards to the people who do that.

Lord Gordon of Strathblane: Do your colleagues want to add a comment? If not, I will follow on with another question that was addressed by a witness in a previous session. Some companies are almost geared to being taken over by one of the biggies. A box is ticked—they are happy. Is there a public interest that should be unhappy? Is there a consumer interest that should be considered, as well as simply the interests of the company being taken over? Is it another three years or another three months?

Robert Colvile: No—it is about three seconds: if you founded a company you can do what the hell you want with it, unless it is illegal.

Lord Gordon of Strathblane: Sorry, you cannot. If it is in the offline world and that company becomes too big, public interest tests start to apply, particularly in your former career in the media. If Rupert Murdoch had anything like the dominance in the newspaper industry that Amazon has in the retail—

Robert Colvile: Yes. That is for government, Andrew Tyrie, the CMA and all the other people to decide. If I start a company and it gets big and Google wants to buy me, yes, the Government have the right to say, "No, we believe this will be harmful to the competition", but you cannot say to me, "No, you should not be seeking to sell your company". That is a very weird position to get into.

Lord Gordon of Strathblane: It may well be. You may be right. If you ran a local newspaper, for example, and wanted to be taken over by a larger local newspaper nearby, the Competition Commission would prevent it. Maybe it should not prevent it, even in the offline world, but can we live with the two worlds coexisting with different rules?

Jamie Bartlett: Mega-tech monopolies in the next 10 years will do incredible harm to democracy but not to consumer welfare. It would be brilliant for consumer welfare but not for the health of democracy. That is the crux of the problem. The monopoly law, based certainly in the US, is obviously based on harm to consumers and particularly prices. Robert is right. It is a fascinating area—working out how you redefine a monopoly if it is not about consumer welfare. While it is potentially a proportion of a share in a very small market—i.e., online advertising—you could say that Google and Facebook in online advertising is something like a duopoly. The proportion of data that you have on users is another issue that people have discussed, as well as cross-industry diversification, as you have mentioned. No one has the answer to it. Many people have tried to work this out. There is not an obvious answer.

The reason I am worried about the future is that the nature of both the internet of things and AI means that the trends that have taken us to Google or Amazon are going to be accelerated for the same reason. It is definitely one that you have to be very careful and worried about. I am not entirely sure I have the answer. If you split Google into two, it would be a less effective and less efficient company. It would not be as good. It is based on having the amount of data that it has.

The Chairman: Mr Laybourn-Langton, is that anywhere the answer?

Laurie Laybourn-Langton: No. We have to break it down by certain functions. The penetration of platforms and apps into transport in an urban environment is vastly different from search engines and other products that Google gives. There is still a response that can be done in particular activities. It would be interesting to explore areas around regulation when you enter certain markets. I believe Facebook has had banking licences in the United States of America for a number of years and is conferred with an enormous competitive advantage because of the data that it holds on many people. It may be that in entering that market officially you would have to, for example, ensure that it has open data so it fits with the open banking movement.

The third point I would make is that having a much more mixed economy of the ownership models around certain platforms could be quite interesting. When it comes to platforms entering these new technology markets, why do we not have state investment banks in the UK that would enable the public sector to invest, to direct technological development and to regain the value? We must remember that many of the technologies that underpin this were developed by state investment in the United States.

The Chairman: Has your point been answered Baroness McIntosh?

Baroness McIntosh of Hudnall: This issue about the undermining of democratic process, which is implicit in some of the answers that particularly Mr Bartlett has given, is extremely important. We have let it go past. It goes back to something that Mr Laybourn-Langton said earlier about relying on democratic process, in a way, to try to create new ways of thinking about how to regulate. If what we are trying to regulate is in the business of undermining the very processes that we are relying upon to deliver that regulation, we are in a vicious spiral. Is there some way we can think about this that does not invite us to go outside and cut our throats? This is very, very challenging. The slightly despairing tone of Mr Bartlett's voice on a number of occasions should not be allowed to go by unnoticed, as it will not show up in the transcript.

The Chairman: Mr Bartlett, can you help us or not?

Jamie Bartlett: Could I get back to you in writing?

Baroness McIntosh of Hudnall: Yes. It would be very helpful.

The Chairman: You have been very thoughtful on this, and further thoughts in writing from any of the witnesses would be very welcome.

Q56 **Lord Gordon of Strathblane:** I have a relatively simple question. We are about to leave the EU, where most of the regulation of the internet takes place. How soluble is the problem that that creates?

Robert Colvile: For me, GDPR is a perfect example of why we are leaving the EU. Equally, we will still be bound by it after we leave. It goes beyond the EU. Jamie mentioned China earlier. The reason the internet has grown and succeeded and has been pretty brilliant, for all its problems—there is enormous happiness, opportunity and wealth—is that it has been a global, open thing that stretches from country to country. One of the difficulties for lawmakers in the UK is that if we go out on our own and say, "We are going to do all these different regulatory things from everyone else", and suddenly the EU starts saying, "We are going to do something different from America", suddenly everything starts to balkanise a bit. I believe three of the 10 largest internet firms in the world are in China. That is a very different model of the internet. It is a much more regulated and state-dominated one. The more the internet balkanises, the more there are different regulatory regimes here and there, the more you lose the connectivity between countries that gives us strength.

Jamie Bartlett: I disagree with Rob on the GDPR. It is a good piece of legislation.

Robert Colvile: You do not run a small business.

Jamie Bartlett: No, but I worked for one. Some of my despairing tone might be slightly helped by some of that. What we are doing in the UK in relation to GDRP, which is basically having it, is a reasonable approach. We will probably try to stay quite closely aligned to what the European Union does on this, and that is probably the right approach. Another area that is very important is that the UK continues to work with the EU when it comes to some of the other colloquial bodies, such as ICAN and the Internet Governance Forum, where a lot of these problems about the fragmentation of the internet are currently unfolding. It is quite important that we work together with other democratic countries on how the internet is regulated.

Laurie Laybourn-Langton: On this particular point, there are costs and benefits of leaving the EU, potentially. If we break away from the power of a regional bloc that has at least tried to resist some of the major platform giants in the world—in which China, at first view, does not necessarily agree with us on certain ideas around liberty and what these platforms should be doing—that could potentially be a very large cost. Alignment with a lot of what is being developed in the EU is probably a very important thing.

I would like to inject a note of optimism in response to Baroness McIntosh's question. We would be particularly interested in ensuring that we slightly break the narrative. It is very important that we see these massive giants like Facebook and Google and we are fixated on them and their activities, rightly so, but we must remember that there are other markets that platforms are penetrating into, or are already in, and others that they will penetrate into. Within that context, we would advocate a much more mixed approach whereby other non-monopolists can be encouraged within those markets. That would create a much more mixed economy model across the piece, enabling us to be less focused on search and other areas which are very dangerous and well-developed into monopolisation, but would also ensure there is a slight counterbalance. One could imagine a situation where you are able to develop some municipal tools for certain regions in the UK that could support the development of democratic engagement that could work as a counterpoint to the power of some of the monopolists as well.

The Chairman: We have run out of time. I am going to take one final question. A number of the members of the Committee are trying to catch my eye. I am going to ask them to let me know their question afterward and we will forward it to you in writing.

Q57 **The Lord Bishop of Chelmsford:** A lot of this has been touched on in the previous answer. I want to ask about new entrants into the marketplace. How can they be enabled to compete with the established platforms, given network effects and some of the other things you have said?

The Chairman: You have touched on it, but if there is anything you would like to add on that—we do want to think about the whole economic impact. Are there any further thoughts you have on entrants into the market?

Robert Colvile: If you wanted to enter the search engine market, you would be an idiot. There are some markets where it is not going to happen. Partly, you hope that there is a chain whereby technology develops as it did previously. Every time we worried about previous dominant companies, a new paradigm came along. There is a counterintuitive issue here, which is that the platforms themselves do spur enormous innovation. AWS, Amazon Web Services, for example, or even the Amazon sales platform itself, have been an immense boon to small and large companies that can use it. You can now literally start a company processing vast amounts of data from your bedroom because AWS will rent you the software power to do it. Whatever we can do to encourage competition and new entrants, we should be doing, which is one of the reasons why I object to the GDPR. Its version of data portability in social networks, for example, is such that it effectively makes it official that no one will ever migrate their social network again. It locks people into Facebook because of the way the provisions work.

Jamie Bartlett: A very specific and simple one is the continued and maybe accelerated efforts by government to make more data that is machine-readable, especially with internet of things devices, transportation data, urban data. Government are one of the largest producers of data. The more they can do to make that available, the more other companies will be able to use that and compete. We are sitting on incredible amounts of data. The NHS is probably the most incredible source of data for medical start-up companies. Anything we can do to encourage that would be a huge positive. That is my optimistic tone.

The Chairman: That is a very interesting point.

Laurie Laybourn-Langton: I would echo that and say that it is potentially a shame that in the development of products using NHS data, we will not have control of what Alphabet DeepMind builds off the back of that. There could have been an alternative situation whereby, by centralising NHS data, the NHS could have had a leveraging position over those who create the products and owned them itself, to ensure that they were developed by other non-Alphabet developers as well. In doing so, that could be linked to the embryonic industrial strategy as well. That is all about determining outcomes in the economy. Outcomes in the economy will be increasingly determined by platforms. Why not have some kind of direction to the development of those platforms?

Baroness Quin: I am struggling somewhat with the statement by Mr Colvile that the GDPR is a perfect reason for leaving the EU, but we are going to be bound by it anyway.

Robert Colvile: I voted remain. I do not like the GDPR.

Baroness Quin: I would like to reinforce the point our Chairman made—if you could send us in writing your thoughts about the consequences of Brexit, the challenges and the possible opportunities resulting from that. Similarly, please put in writing to us your thoughts about the international dimension for the future: whether there are international bodies we ought to be trying to increase involvement with, or whether there is a gap for new international bodies—particularly given the points about China and so on—and how you see that international dimension carrying forward into the future.

The Chairman: We are going to ask you to respond in writing to that. We have had a very interesting session. You have given some perspectives on the subject that we have not had from previous witnesses. Of course, there are some concerns, but we have had quite a bit of clarity on some aspects of regulation that we have not had before and we welcome and appreciate it. The clerk will write to you and ask you to respond to Baroness Quin’s questions on Brexit and to some further questions that we would have liked to ask on personal data and how it is handled. If you would be kind enough to respond to us either specifically or by sending us other material, we would appreciate it.

May I thank our witnesses for their time today? It has been illuminating. We would have liked two hours with you, so you can maybe come back some other day. Thank you very much indeed.

Centre for Policy Studies – supplementary written evidence (IRN0111)

Answers to additional questions from the oral evidence session on 29 May 2018

DATA PROTECTION

Question 6

a. What information should online platforms provide to users about the use of their personal data? How should it be presented?

Online platforms should handle the personal data of users transparently. It should be presented in a sufficiently simple format to enable users to accurately assess what data is held on them, and how it will be processed and this information should be clearly signposted on the platform.

Online platforms should inform users if their personal data will be shared or sold on to a third party - the recent case where the company 'Emma's Diary' sold personal data relating to new mothers to the Labour Party to be used in the General Election 2017 highlights why this is a necessary provision.

b. Does the GDPR, in your view, provide sufficient protection for individuals in terms of transparency in the collection and use of personal data or do we need further regulation?

The GDPR has, in many ways, been a textbook example of how not to do it. The GDPR has created widespread confusion in businesses not only in the UK but around the world, with a recent survey reporting 44% of participating companies fearing they could lose revenue as a result of non-compliance.[585] It's also made surfing the internet a much more aggravating experience – and in many ways serves to increase the dominance of large platforms over smaller rivals, for example via the restrictions on data portability which mean that you cannot export your social graph to another site. (Ben Thompson of Stratechery is very good on this.)

INTERNATIONAL REGULATION OF THE INTERNET

Question 7

a. What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

Whilst the United Kingdom remains part of the European Union, including the duration of the transition period, the GDPR will remain fully enforceable on

[585] https://www.econsultancy.com/blog/69945-companies-around-the-world-are-worried-about-the-gdpr-study

British soil. Yet upon the United Kingdom's exit from the European Union, GDPR will continue to apply in many instances, given that is has extra-territorial applicability – and that few businesses are going to want to run their operations according to two separate sets of regulations.

There is, as we discussed, a paradox here – one of the advantages of leaving the EU is that we can set our own regulations, but equally it is vital economically and indeed politically that the internet, or at least the Western internet, continues to operate according to a set of shared values and standards, rather than Balkanising into separate zones.

It is obviously less than ideal that Britain will no longer be in a position to temper many of the EU's instincts – its embrace of the preventative principle in particular tends against economic dynamism. But much of the internet's governance is on a global basis. Also, Britain was already pledged – via the Conservative manifesto – to police internet speech and behaviour more vigorously than before, which is an area that operates largely outside of international regulation, although cooperation with other countries is of course frequently required.

Whilst it is important that the United Kingdom remains vocal in the global discussion on internet regulation and continues to co-operate with international bodies such as the UN or OECD, it is important that the UK is emboldened to regulate as a sovereign nation in this policy sphere.

By acknowledging that the one-size-fits-all approach that the GDPR enforces is not appropriate for internet regulation and adopting a more flexible and proportionate approach, the UK will be able to foster a regulatory environment which protects individuals and opportunities for enterprise in equal measure.

b. What other international bodies should the UK work through to improve internet regulation?

The UK should continue to work through the array of specialist bodies that currently exist. The UK is currently and will remain an important voice in the global internet regulation debate. If we begin to advocate for measures that undermine this multi-stakeholder framework and move us towards a state-by-state regulatory approach, this will only embolden those countries who seek to normalise state regulation of the internet.

July 2018

Centre for the Analysis of Social Media at Demos, Centre for Policy Studies and Institute for Public Policy Research – oral evidence (QQ 52-57)

Transcript to be found under Centre for Policy Studies

Centre for the Response to Radicalisation and Terrorism, The Henry Jackson Society - written evidence (IRN0093)

About The Henry Jackson Society

The Henry Jackson Society (HJS) is a London-based think-tank founded on the global promotion of the rule of law, liberal democracy, and civil rights. HJS specialises in the study of international terrorism, counter-terrorism, and radicalisation.

About the Centre for the Response to Radicalisation and Terrorism (CRT)

CRT is unique in addressing violent and non-violent extremism. By coupling high-quality, in-depth research with targeted and impactful policy recommendations, we aim to combat the threat of extremism in our society.

About the Author

Nikita Malik is the Director of the Centre for the Response to Radicalisation and Terrorism at The Henry Jackson Society. She holds an MA in Economics and an MSc in South Asian Studies from the University of Oxford, and an MSc in Middle Eastern Politics and Arabic from SOAS, the University of London. Malik's research focuses on combatting Islamist and Far Right extremism in the UK. She has advised SO15 Counter Terrorism Command, the National Crime Agency, the EU Radicalisation Awareness Network, the Department of State, the United Nations, Google, Facebook, and others on issues related to extremism and terrorism.

Summary of this submission

- Any effective regulation of the internet will need to be tailored to address its specific areas: the surface web, deep web, or darknet.

- More national and international cooperation will be required to determine legal liability of those who abuse the internet.

- While self-regulation by technology companies is an ideal solution in monitoring and removing hateful or harmful material off the internet, self-regulation has failed in the sense that this material continues to appear and germinate on the internet.

- If resources to expand and include the supervisory powers of existing bodies are insufficient, an external body of experts (the Internet Regulatory Body) should be appointed with the role of regulating, scrutinising, and auditing the efforts of technology companies to remove extremist content and instructional terrorist content.

1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

a. It is not possible to regulate the internet without focusing on its specific areas. The internet can be broken down into three parts:

i. The 'surface web', which is used by all internet users, and contains information and websites accessed by using standard search engines like Yahoo, Google, or Bing.

ii. The 'deep web', which is approximately 400 to 500 times larger than the surface web,[586] and contains certain user restrictions when it comes to access. Though internet users use the deep web regularly, its data is generally accessible through application programming interfaces (APIs) in which the user is granted access to the required database.[587] Internet sites such as Facebook, Twitter, or Snapchat, for example, as well as file-sharing services such as Dropbox, Google Drive, Webmail, and online banking pages, are part of the deep web because they require verified logins before access is granted.[588]

iii. The 'darknet', which exists within the deep web but is even harder to access, and is largely unregulated. The darknet contains a smaller portion of information stored on the internet[589] and is, effectively, a repository of 'hidden' sites accessible through uniquely downloadable software programmes that support encryption.[590]

iv. Specific regulation of the internet will be determined by *which part* of the internet is under examination. Areas such as the surface web, for example, will require regulation spearheaded by technology companies or platforms that publish information, while information on the darknet will be harder to regulate and will fall on human intelligence institutions and the police to monitor, capture, and remove material.

b. When it comes to the issue of national security threats, evidence does not reveal wide-scale use of the internet by terrorists and extremists, and the evidence presented of this use is limited[591]. However, case studies indicate that, unless appropriately addressed, emerging trends may burgeon into major challenges for the Government in the future:

[586] Bergman M. K., 'White Paper: The Deep Web: Surfacing Hidden Value', *Journal of Electronic Publishing* 7.1 (2001), last visited: 24 October 2017.

[587] Chertoff, M., op. cit., p. 27.

[588] Chertoff, M., op. cit., p. 27; Egan, M., 'What is the Dark Web, What is the Deep Web, and How Can you Access it?' *Tech Advisor*, 10 October 2017, available at: http://www.techadvisor.co.uk/how-to/internet/dark-web-3593569/, last visited: 14 November 2017.

[589] Egan, M., op. cit.

[590] Moore, D., Rid, T., 'Cryptopolitik and the Darknet Survival' *Survival: Global Politics and Strategy* Vol. 58 (1), (2016): pp. 7-38. Encryption is understood as the act of "scrambling communication to prevent access to others apart from the intended recipient". For more, see: Titcomb, J., 'What is Encryption, how does it work and what apps use it' *The Telegraph*, 29 March 2017, available at: http://www.telegraph.co.uk/technology/0/encryption-should-using/, last visited: 13 September 2017.

[591] See, for example, Malik, N. (2018), "Terror in the Dark: How Terrorists Use Encryption, The Darknet, and Cryptocurrencies". *The Henry Jackson Society.*

i. The first challenge is that extremist content and instructional terrorist material, as well as funding campaigns to raise money for terrorist groups, can be found on all parts of the internet – with varying degrees of accessibility.[592] While some of these issues have been addressed in the UK by the 2016 Investigatory Powers Act, there remains work to be done to further research on extremism and terrorism on the darknet and understand its links to, and overlap with, the surface web. This will have a direct effect on the remit of regulation.

ii. The monitoring of instructional terrorist material on the darknet, and how criminals and terrorists may use funding to drive document fraud, guns, and proceeds from drug sales, will require the cooperation of diverse approaches of national cyber security. The NCA and GCHQ set up a specialist unit to look at the darknet in 2014.[593] While this focuses on child abuse, similar coordination can be used to examine terrorism, and feed into regulation. More resources should be dedicated to JTAC in coordinating intelligence approaches on policing online markets, using human intelligence to monitor activity.

iii. Moreover, terrorist funding campaigns such as those seen on the deep web and on the darknet involving bitcoin and other cryptocurrencies should fall under the remit of the new Anti-Money Laundering Watchdog,[594] and JTAC can work with this body to disrupt financial flows to terrorist and extremist groups.

c. Therefore, regulation of the internet will only be possible with the cooperation of multiple government agencies, bodies, and private sector companies, particularly when it comes to regulation to remove harmful or hateful material, and content that threatens national security.

2. What should the legal liability of online platforms be for the content that they host?

a. The question of assigning what should be the legal liability of online platforms for the content they host is secondary to determining how best to deal with unacceptable online content, particularly that of an extremist and/or illegal nature.

b. The removal of extremist and terrorist content from the surface web, deep web, and darknet – particularly in the case of artificial intelligence programs that may do ‘bulk’ removals - creates a risk that evidence needed for prosecution of individuals disseminating content or providing material support to terrorist organisations may be lost. Technology companies should

[592] Malik, N. (2018), “Terror in the Dark: How Terrorists Use Encryption, The Darknet, and Cryptocurrencies”. *The Henry Jackson Society.*

[593] Watt, N., ‘’Dark Web’: GCHQ and National Crime Agency join forces in hunt for child abuse’, *The Guardian,* 11 December 2014, available at: https://www.theguardian.com/society/2014/dec/11/gchq-national-crime-agency-dark-web-child-abuse, last visited: 28 February 2018.

[594] For more, see: Glen, J., ‘UK launches new anti-money laundering watchdog’, *HM Treasury,* 23 January 2018, available at: https://www.gov.uk/government/news/uk-launches-new-anti-money-laundering-watchdog, last visited: 21 February 2018.

work with law enforcement to ensure that this material is not simply removed, but archived effectively to understand patterns of behaviour.

c. Further complicating ambiguities of any auditing process is legal interpretation. More than ever, there is a need for legislation to understand context, intent, and anonymity in cases of prosecution of those disseminating extremist or terrorist content online, including, but not limited to, Section 2 of the Terrorism Act 2006[595] and Section 58 of the Terrorism Act 2000[596].

d. Therefore, greater transparency is required on government definitions of terrorism and extremism for legislative purposes[597], particularly on definitions of terrorism online. Given there is no comprehensive international legal definition of terrorism[598], and the internet is a global space, more international cooperation is recommended regarding the responsibility of prosecution.

e. The limited number of prosecutions against individuals promoting terrorism on the internet suggests a lack of effectiveness[599], however, better evidence gathering online can help form an understanding of profiles, groups, and networks disseminating extremist or terrorist content on multiple platforms to feed into national court systems and auditing processes.[600]

Recommendations to policy makers for potential future regulation

a. The existing powers and regulations available in the United Kingdom to audit and regulate the internet are unclear. Further complicating the matter is the fact that companies such as Google and Facebook operate as quasi-monopolies and enjoy dominant market positions.

   i. The first, and most desirable option when it comes to moderating content, is to apply greater pressure on these companies to promote, implement, and approve a self-regulatory model where transparency and accountability of the removal of extremist content hosted on these

[595] *Terrorism Act 2006,* United Kingdom of Great Britain and Northern Ireland (2006), Chapter 11, Section 2, available at: https://www.legislation.gov.uk/ukpga/2006/11/section/2, last visited: 14 February 2018.

[596] *Terrorism Act 2000,* United Kingdom of Great Britain and Northern Ireland (2000), Chapter 11, Section 58, available at: https://www.legislation.gov.uk/ukpga/2000/11/section/58, last visited: 14 February 2018.

[597] **Anderson, D., 'Attacks in London and Manchester March-June 2017' Independent Assessment of MI5 and Police Internal Reviews, (2017), available at:** https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/664682/Attacks_in_London_and_Manchester_Open_Report.pdf**, last visited: 11 January 2018.**

[598] Will become harder to prosecute as individuals are not in physical territory, but online, meaning allegiances will be harder to find – and must be consistent with international human rights definitions about freedom of speech and right to consume information.

[599] Walker, C., 'The War of Words with Terrorism: An Assessment of Three Approaches to Pursue and Prevent' *Journal of Conflict and Security Law* Vol. 22(3) (2017), available at: https://academic.oup.com/jcsl/article-abstract/22/3/523/4554473?redirectedFrom=fulltext, last visited: 11 January 2018.

[600] See Malik, N. (2018), "Terror in the Dark: How Terrorists Use Encryption, The Darknet, and Cryptocurrencies". *The Henry Jackson Society.*

platforms is made publicly available through the publication of an annual report.

ii. Such reports should reference statistics on content flagged by users, outcome of investigated content, decision-making systems employed by these companies on content removal, case studies, and areas for improvement.

iii. Transparency will further incentivise technology companies to cooperate in this field, and has the potential to foster further innovation in the successful removal of extremist and hate content.

b. Surface Web

i. The public should be able to report and flag extremist content found the surface web to those companies hosting such content.

ii. For example, there is still no 'flagging' system for users to report instructional terrorist manuals or disturbing extremist content on Google search results, with software often auto-predicting extremist literature or directing vulnerable people who may consume this content to more extremist literature (in multiple languages).

iii. An example of a solution could be the creation and dissemination of trusted third-party programs for platforms like Google, and other search engines, to make such extremist material less visible.[601]

c. Deep Web

i. Self-regulation mechanisms should also be applied by technology companies such as Facebook and Twitter, who have an equivalent social responsibility towards their users.

ii. Again, annual reports on internal auditing mechanisms should be made publically available, bolstered by online reporting mechanisms involving the public.

d. Darknet

i. The Government should lead campaigns to deconstruct myths around the darknet.

ii. The 2017 report by David Anderson QC, the former Independent Reviewer of Terrorism Legislation in the UK, indicated a new

[601] See Malik, N. (2018), "Terror in the Dark: How Terrorists Use Encryption, The Darknet, and Cryptocurrencies". The Henry Jackson Society.

commitment by MI5 to allow knowledge derived from intelligence to be shared more widely beyond intelligence circles. [602]

iii. Building and sharing intelligence capital in this way will help to deconstruct myths on the darknet, by providing explanations and evidence on its use.

iv. GCHQ can also share knowledge with ordinary researchers and universities to train them on understanding internal darknet hidden market communities, as well as on regulation and the code of conduct for intelligence gathering.

e. While a self-regulatory model to remove and audit extremist content is an ideal solution, it has yet to be realised to date. Extremist content is still widely available online, and there remains further work to be done by technology companies to remove this material.[603] If such self-regulation continues to fail, the need for a regulatory body to supervise and assess the efforts of these technology companies in this space only grows.

f. The debate on whether the existing supervisory powers of the Office of Communications (Ofcom) can be expanded to achieve the above depends on whether social media companies can be classified as publishers. While this presents a potential solution, it requires a change in classification, and the lack of resources available to Ofcom may mean that such regulation is not possible[604].

g. **If resources to expand and include the supervisory powers of existing bodies are insufficient, an external body of experts (the Internet Regulatory Body) should be appointed with the role of regulating, scrutinising, and auditing the efforts of technology companies to remove extremist content and instructional terrorist content.**

i. The Internet Regulatory Body must first review the efforts of social media companies to self-regulate content off their own platforms, with the potential for fines being placed on those companies that consistently fail to remove instructional terrorist material, material support campaigns that fund terrorism, or propaganda shared by proscribed terrorist organisations and preachers within a certain timeframe.

[602] **Anderson, D., 'Attacks in London and Manchester March-June 2017', Independent Assessment of MI5 and Police Internal Reviews, (2017), available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/664682/Attacks_in_London_and_Manchester_Open_Report.pdf, last visited: 16 January 2018, p.33.**

[603] See Appendix 1 of Malik, N. (2018), "Terror in the Dark: How Terrorists Use Encryption, The Darknet, and Cryptocurrencies". The Henry Jackson Society.

[604] Mayhew, F., 'Lord Burns tells MPs Ofcom would be "suitable vehicle" to regulate social media as he is approved next chairmain', *PressGazette*, 13 December 2017, available at: www.pressgazette.co.uk/lord-burns-tells-mps-ofcom-would-be-suitable-vehicle-to-regulate-social-media-as-he-is-approved-next-chairman/, last visited: 21 February 2018.

ii. Fines can follow the model of breaching UK competition law[605] and the Internet Regulatory Body should work closely with the Counter Terrorism Internet Referral Unit (CTIRU) and other existing regulatory bodies, to achieve this. Part of the auditing process should include regular annual reports, which measure key metrics on compliance and reflect on areas of improvement, and are available to the public.

iii. Money created from potential fines on companies that fail audit reviews can potentially be used to fund intelligence capital on crime and terrorism on the darknet. This can involve funding research and analysis of marketplaces on the darknet, the use of cryptocurrency and encryption by terrorists, and learning how to infiltrate, study, examine, and source terrorist content and data into an archive for researchers and law enforcement who need to refer to this material.

May 2018

[605] Firms involved in anti-competitive behaviour, including abuse of a dominant market position, risk being fined up to 10% of group global turnover. Anti-competitive behaviour within the UK is specifically prohibited by Chapters I and II of the Competition Act 1998 and the Enterprise Act 2002. However, it should be noted that fines are fiscally complicated. For more, see: 'Competition law – the basics', Out-Law.com, April 2014, available at: https://www.out-law.com/en/topics/eu--competition/competition/competition-law---the-basics/, last visited: 13 March 2018; 'An overview of the UK competition rules', Slaughter and May, June 2016, available at: https://www.slaughterandmay.com/media/1515647/an-overview-of-the-uk-competition-rules.pdf, last visited: 13 March, 2018; Titcomb, J., 'Google hit with record £2.1bn EU fine for abusing internet search monopoly', *The Telegraph,* 27 June 2017, available at: https://www.telegraph.co.uk/technology/2017/06/27/eu-hits-google-record-21bn-fine-abusing-internet-search-monopoly/, last visited: 13 March 2018.

Channel 4 – written evidence (IRN0105)

1. Introduction

Channel 4 welcomes the opportunity to respond to the Communications Committee's inquiry into Internet Regulation. The Internet has had a transformational effect on both our society and economy and has brought with it great advantages. However, it has become increasingly apparent that in the online world legislation has failed to keep pace as digital online platforms have grown rapidly, unchecked, despite their increasing importance and influence in our everyday lives.

The lack of regulation has led to the emergence of a duopoly in the form of Facebook and Google which has distorted the marketplace. Insufficient regulation and the unchecked dominance of these two global players in particular, has surfaced a number of important societal and industry issues such as fake news and misinformation, data misuse, extremist content, ad fraud and brand safety, all of which need to be addressed as a matter of urgency.

This is in contrast to public service broadcasting in the UK, which exists to serve society and support the creative industries, has best in class regulation and sets a benchmark in terms of trust and standards. In an era where British democratic values are being tested, the high-quality, trustworthy journalism provided by broadcasters matters more than ever. Public service broadcasting continues to be a beacon for trusted impartial information but the playing field needs to be more even to ensure that consumers are protected and so that broadcasters can compete on a fair basis as it is increasingly evident that the digital deck is significantly stacked against us. Channel 4 believes that it is vitally important that industry and policymakers act now to address the unregulated power of tech platforms given the potentially harmful implications posed.

2. About Channel 4

With a mission to innovate, be diverse, present alternative views and stimulate debate, Channel 4 is required to take risks and challenge the status quo. As a publicly-owned, but entirely commercially-funded public service broadcaster, Channel 4 sits as a unique hybrid alongside the BBC, ITV and Channel 5. This model ensures that Channel 4 operates free from both commercial and political influence, as a broadcaster that is not shareholder-owned but which also operates at no cost to the British taxpayer. Under this model, Channel 4 puts its profits back into programmes, with the ultimate objective of delivering its statutory remit and specific Ofcom licence obligations. Combined with Channel 4's status as a "publisher broadcaster", which means all of its commissioned programmes are made by external production companies, Channel 4 is an agile and innovative "challenger brand" in the creative industries.

Channel 4's detailed statutory public service remit includes requirements to produce high quality news and current affairs; to support and stimulate well-informed debate on a wide range of issues, including by providing access to information and views from around the world; as well as requirements to challenge established views and promote alternative views and new perspectives.

In recent years, there have been significant changes to the UK media with the increase in competition through digital switchover and the rise of online platforms. Despite the rise in digital and online, TV has remained remarkably strong and Channel 4 has had a proud history of innovation in this space. Channel 4 was the first broadcaster in the world to launch a VOD service – 4oD in 2006 – which 12 years later has evolved into All 4. As well as being the first to launch an on demand service Channel 4 was also the first to register viewers online which was launched alongside our award winning viewer promise and enables us to tailor programme recommendations and deliver relevant advertising to viewers. All 4 now has over 16 million registered users including two thirds of all 16-34 year olds in the UK, demonstrating Channel 4's ability to reach audiences across different platforms and compete with other online services. All 4 continues to grow and digital is now a £100m a year business with 24% growth in our digital revenues last year.

Furthermore, Channel 4 has been an innovator on social media. Our expansion onto these online platforms signals our strategy to engage young people with serious, credible, trusted content on the platforms they are increasingly using. In 2017, videos across the *Channel 4 News* portfolio received 1.98 billion views across Facebook and YouTube[606]. In addition, *Unreported World* now has its own YouTube channel, with new videos being uploaded weekly – with some videos garnering in excess of one million views. Building on the success of *Channel 4 News*'s video content on social media, Channel 4, E4 and All 4 have also experienced explosive growth on these platforms this year. This has resulted in Channel 4 being ranked 47th globally for social video at year end – higher than much bigger organisations such as Netflix, Amazon, ITV and Sky as well as key challenger brands such as Vice.

It was a record-breaking year for our pages on social media, with our entire network's video content being viewed over 6.5 billion times across Facebook, Instagram and YouTube – this is more than double the number in 2016[607]. However our ability to continue to deliver this kind of impact is entirely at the whim of the platforms who can drastically reduce our reach with just a change of their algorithm.

3. Challenges posed by online platforms

Whilst the internet has unquestionably transformed how people around the world communicate, gather information and consume educational and entertaining

[606] Channel 4 2017 Annual Report
[607] Channel 4 2017 Annual Report

content[608], the scale and pace of this technological change has also presented many challenges due to the lack of regulation compared to traditional media.

3.1 Fake News and Data Misuse

There are societal concerns caused by the lack of regulation online such as the proliferation of misinformation or 'fake news' and the misuse of personal data. These need to be taken seriously due to the potential for both these areas to be manipulated to influence people's decisions, the propensity for fake news to be spread easily, widely and instantaneously online and the impact that both can have on democracy.

Fake news first emerged as an issue following the US election - Buzzfeed research found that in the final three months of the US presidential campaign, the top-performing fake election news stories on Facebook generated more engagement than the top stories from major news outlets such as the *New York Times*, *Washington Post*, *Huffington Post*.[609]

One of the key concerns is the impact this could have on young people, who are increasingly consuming news through online platforms. Whilst Ofcom research shows that TV remains the most popular news platform in the UK and is used by over two thirds (69%) of adults for news - double that of adults consuming print news (31%) and radio (32%) and greater than those who claim to use the internet for news (41%). But this is almost inverse for 16-24s, who are more likely to use the internet or apps for news than TV (59% of 16-24s)[610]. Millennials are also more likely than previous generations to use digital devices to access news which gives them the freedom to 'snack' on small but frequent bits of news throughout the day that they integrate with their daily activities[611].

The increased take up of these digital devices amongst younger consumers comes at a time in which anybody can become a publisher. Indeed, social media has become increasingly influential in how people access news, spurred on by a consumer appetite for tailored content. However, social media platforms are able to tailor this content through the use of algorithms which predict what information they believe users would like to see[612]. On sites such as Facebook and Twitter, this content can be based on information such as their interests, location and past-click behaviour or what is 'trending'. This has led to the creation of "filter bubbles" where news feeds use algorithms that direct users to content that echoes and reinforces their own views. While headline grabbing fake news articles can become popular and have a 'snowball effect' online reaching millions of users. This problem is further exacerbated by the inability or

[608] House of Lords Select Committee on Communications: The Internet: To Regulate or Not To Regulate? Call for evidence https://www.parliament.uk/documents/lords-committees/communications/InternetRegulation/Internet-regulation-call-for-evidence.pdf

[609] Source: BuzzFeed - https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm_term=.eo5ZoJRvm#.wy2zR16PM

[610] Source: Ofcom News Consumption research, 2015

[611] Source: Newsworks, 2015: http://www.newsworks.org.uk/Topics-themes/generation_news/78136

[612] Source: John Nicolson Report for Channel 4, 2017

unwillingness of social media platforms to put sufficient resource behind identifying and removing fake news.

It is therefore unsurprising that research conducted by YouGov for Channel 4 shows that concern about fake news is more acute among young people, with 57% of 18-34 year olds stating they are worried about fake news - compared to 49% of UK adults.[613] The survey also found that in practice people find it difficult to distinguish fake news from real news stories. When those surveyed were shown six individual news stories, three of which were true and three of which were fake, only 4% were able to correctly identify them all correctly. In addition, despite half (49%) of respondents to the survey stating they were either 'very or fairly confident' that they could tell the difference between a fake news story and a real news story, half of this group believed at least one of the fake news stories shown.

There have been a number of high profile investigations which have demonstrated that the digital giants are either unwilling or unable to effectively police their platforms and remove content which would be unacceptable on any other medium. The platforms state that they are mere conduits and are not responsible for the content users upload to their platforms. Whilst Channel 4 does not believe it would be proportionate or practical to expect these platforms to pre approve all content which appears on their platforms, they should take a far greater level of responsibility for policing and moderating their platforms to ensure that illegal content or blatant misinformation is removed immediately.

The recent Cambridge Analytica / Facebook data scandal exposed by Channel 4 News and the Guardian revealed that the personal information from over 87 million Facebook users was covertly harvested by the data analytics firm who used the data to target citizens in an attempt to influence democratic elections. It also highlighted severe shortcomings in Facebook's approach to user data, privacy and transparency and the pressing need for increased accountability.

Channel 4 believes that transparency about what businesses do with user data and the provision of clear controls for users are essential. Channel 4 is clear about the permissions that it asks for on our digital service All 4 and how we use that data to tailor both the advertising and the programming users see. We also ensure users are in total control of their data and are able to delete it at any time. In 2016, Channel 4 won the Mediatel Grand Prix prize, as well as Best Use of Connected Data, for our 'Ad4You' initiative, which judges praised as an "excellent example" of using consumers' personal data responsibly and effectively for advertising. Our ethical and transparent approach to data has also been used as a case study in the Harvard Business Review (May 2015).

3.2 Continued Importance of Public Service Broadcasting

As providers of high quality, trusted and impartial News and Current Affairs, Public service broadcasters still play a vital role to ensure that the public has access to content that can inform debate rather than distort it. The UK is a case

[613] Source: YouGov survey of 1684 British adults aged over 18 commissioned by Channel 4, January 2017

in point of the benefits of a sophisticated broadcasting ecology in providing trusted news. The UK system is underpinned by a strong public service broadcasting core comprising a variety of organisations with different models, missions and purposes which serve the British public with a wide range of public service programming – from the publicly owned and publicly funded BBC, through to commercial providers such as ITV and Channel 5. Two other elements of the UK's public service broadcasting system underpin its world- renowned status for high-quality and trusted news. Firstly, an independent system of regulation overseen by Ofcom, with strict rules on accuracy and due impartiality and other detailed content standards as set out in Ofcom's Broadcast Code. As broadcasters are licensed, this means that regulators have real powers to sanction those broadcasters behaving inappropriately – and indeed Ofcom have utilised this power in the past through fines and even the ultimate sanction of removing a licence to broadcast, as was the case of Press TV[614]. Secondly, a clear set of quotas and requirements for the provision of high quality news and current affairs.

Within this, Channel 4's distinctive public service remit, outlined above, ensures that Channel 4 News takes a different approach to news coverage than other broadcasters and is known for its risk-taking, high-impact, agenda-setting journalism. The investigative approach of Channel 4 News, which was recently awarded its third international Emmy for News in five years for its coverage of the Syrian Civil War, also has an important impact in society, public life and the wider world. Notable investigations include its recent investigation into allegations of child abuse at Christian camps, its investigation into Amazon's website recommending bomb making ingredients, exposing exploitation of migrant employees involved in fruit packing for major British supermarkets and its investigation into Bupa care homes. The impact of our journalism highlights that the point that freedom of speech and regulation can go hand in hand.

3.3 Advertising

The health of the UK's advertising market plays a vital role in ensuring the ongoing success of UK television, UK made content creation and the overall UK economy. However, Channel 4 believes that that the current digital media market is far from fair, open and competitive. Facebook and Google are an unregulated duopoly who dominate the market - commanding 84% of global spend in 2017[615]. In any other market they would be subject to a high degree of regulation but in the UK the lack of regulation enables them to leverage their market power unchecked. Channel 4 believes that this lack of regulation has led to a multitude of issues including brand safety and illegal content, ad content standards, ad fraud and measurement.

3.3.1 Ad Content Standards

As noted above, Broadcasters operate in a strict regulatory environment in terms of the standards which apply to the content they can show. Broadcasters are also subject to strict regulations around the advertisements that can appear

[614] https://www.theguardian.com/media/2012/jan/20/iran-press-tv-loses-uk-licence
[615] https://www.marketingweek.com/2017/12/05/ritson-digital-duopoly-2018/

around the content they broadcast. In addition, Channel 4 voluntarily apply the BCAP advertising code with its higher levels of consumer protection to advertising on our online service All 4, as we believe this is the most appropriate and responsible position. These restrictions were put in place with the aim of protecting children from inappropriate adverts but despite the increase in the number of young viewers watching content on platforms like YouTube and Facebook, there is not the same standard of regulation online.[616]

3.3.2 Illegal Content and Brand Safety

Both Google and Facebook have also failed to sufficiently protect the brands which advertise with them; placing adverts for popular supermarkets, soft drinks and sportswear brands against highly inappropriate, sometimes illegal content. By doing so they are not just damaging those brands and financially supporting the people who upload these videos, but they are also profiting from them.

A Times investigation recently found that some of the world's biggest brands were unwittingly advertising against inappropriate content of children. One of these Channels whose videos often depicted children in abusive situations grew to one of the top 100 most viewed Channels on YouTube with 8.53m subscribers. Its content was flagged several hundred times before it was finally removed having generated £7.1m/year for Google.

The issue of inappropriate content on YouTube is widespread, including on its supposedly safe YouTube Kids app[617]. YouTube recently announced it had removed ads from nearly 2 million videos and over 50,000 channels which were masquerading as family-friendly content. Whilst their efforts to protect brands by removing the adverts from these videos are welcome, the fact that YouTube has failed to remove the content itself, leaving children unprotected, demonstrates that there is a significant problem. This came to a head in 2017 when several major brands including Channel 4 as well as Adidas, Mars, HP, Diageo, Cadbury, Lidl and Deutsche Bank amongst others, removed their campaigns from YouTube in protest. This is in contrast to the security provided by our on demand service All4 as Channel 4 voluntarily applies the same strong advertising rules across linear and online – ensuring children enjoy the same protections when viewing our content online as they do offline. Furthermore, the broadcast market is subject to tight regulation of content through the Ofcom code.

3.3.3 Ad Fraud

Ad fraud is highly prevalent in the online ecosystem and is a problem associated with the unregulated automated ad trading on these digital platforms. The majority of ad fraud occurs when rogue publishers create bots to visit their websites to falsify high volumes of traffic[618]. As a result, brands and advertisers do not get the reach, views and clicks they pay for. There are clear differences in the quality of the advertising environment between broadcasters and online as

[616] https://www.nytimes.com/2015/11/25/technology/youtube-kids-app-faces-new-complaints.html
[617] https://www.nytimes.com/2017/11/04/business/media/youtube-kids-paw-patrol.html?_r=0
[618] Thinkbox's written evidence to the Communication Committee's Inquiry on The Advertising Industry

adverts on television and on broadcasters' digital services are completed ads, full screen and watched by humans. This is in contrast to the rest of the digital universe where the Media Ratings Council counts 2 seconds as a view and where consumers can simply scroll past adverts with the audio often muted.

Strikingly, a report by Business Insider estimated that the amount of global advertising revenue wasted on fraudulent traffic, or clicks automatically generated by bots was estimated to have reached $16.4 billion in 2017[619]. A recent example of the issues with ad fraud has also recently seen with the dozens of fake adverts featuring the consumer advice expert Martin Lewis on Facebook[620].

3.3.4 Measurement

Furthermore, whilst TV has a best in class system for measuring the reach and effectiveness of advertising through the BARB panel, online has a patchwork of companies with no accepted common standards and platforms often 'mark their own homework'. This has resulted in Facebook frequently having to admit it has overstated and artificially inflated its ad metrics. In 2017, it said it could reach more young people than actually exist in UK, US, Australia, Ireland and France[621] while in the UK, Facebook claimed to reach 12.2m adults aged 20-29, despite the population in this age group being just 8.76m.

4. Areas to address

Television is one of the most regulated mediums in the world, and this regulation has been put in place precisely because of the influential role TV plays. Channel 4 believes that this regulation is entirely appropriate, has been carefully considered and is evidence based. It ensures that British Television offers a gold standard and a safe environment for families to view content. However, the same cannot be said for the online world where legislation has failed to keep pace as digital online platforms have grown rapidly, unchecked, despite their increasing importance and influence in our everyday lives.

Channel 4 believes it is essential that this imbalance is corrected to ensure citizens are protected against some of the issues laid out in this paper and to ensure organisations like Channel 4 can operate on a level playing field.

Channel 4 believes that policy makers should take a multi-pronged approach to addressing these issues.

- The Government should consider what options it has available to strengthen areas of the UK's creative industries which can serve to counteract issues like Fake News. Chiefly Channel 4 believes the Government should urgently strengthen the PSB prominence regime.

[619] http://uk.businessinsider.com/ad-fraud-estimates-doubled-2017-3?r=US&IR=T

[620] https://www.theguardian.com/technology/2018/apr/22/martin-lewis-sues-facebook-over-fake-ads-with-his-name

[621] https://www.theguardian.com/technology/2017/sep/07/facebook-claims-it-can-reach-more-people-than-actually-exist-in-uk-us-and-other-countries

- The Government should consider a wide range of regulatory remedies that address the both the lack of transparency and accountability of large online players like Facebook and Google.

- There should be greater scrutiny of the size and dominance of these players in relation to the digital advertising market, to ensure they are not distorting the market, harming competition and consumer choice. This could include a review by the Competition and Markets Authority, for example.

4.1 Prominence of Public Service Broadcasting

Given the important role PSBs can play as a counterweight to the prevalence of fake news and misinformation, Channel 4 believes that policymakers should urgently update the current prominence regulations to ensure viewers can continue to find impartial, trustworthy content.

One of the biggest challenges for Channel 4 and for public service broadcasting in the years ahead will be ensuring viewers can continue to find our content. Public service broadcasting is vital to our culture, our democracy and the continued global success of our creative industries. But it is a system that needs to be supported and nurtured to ensure it can continue to compete with the dominance of global players. Prominence is the cornerstone of the public service broadcasting compact – ensuring audiences can easily find the public service content Parliament have asked us to produce and ensuring commercial public service broadcaster like Channel 4 can continue to fund that content by attracting large enough audiences is essential. It is important that policymakers consider the discoverability of the content PSBs are being asked to produce, particularly as viewing habits change.

Channel 4 believes that the existing prominence rules are no longer fit for purpose and are constantly being undermined by online and pay platforms. The rules are strictly limited to the linear EPG and take no account of how viewers are increasingly accessing content in different ways. For example, while All 4 contains all of the content aired on Channel 4 it receives no guarantee of prominence. The linear EPG itself is increasingly difficult to find with smart TV manufacturers and pay TV platforms in particular pushing users towards unregulated areas of their platforms where they disaggregate content and can promote their own content or the content of organisations that pay for the privilege. Meanwhile organisations like Netflix and Amazon are increasingly requiring manufacturers to include a dedicated button on their remote control. If PSBs are to be able to continue to compete it is essential that the rules are updated to ensure they are fit for purpose as viewers increasingly access content in different ways.

4.2 How policymakers should approach regulation online

Channel 4 believes that viewers expect the same level of protections to apply online as they do offline. At minimum this should mean that online platforms like YouTube and Facebook take responsibility for properly managing their platforms and remove content that would be unacceptable anywhere else. Given the scale and influence of companies like Google and Facebook[622] Channel 4 believes that they must be made to take more responsibility and invest more to develop solutions to these issues.

It is clear that self-regulation has proved insufficient to tackle the issues raised, with platforms failing to take responsibility even where there is clear societal harm. Indeed while Mark Zuckerberg has now admitted Facebook should be subject to regulation – he appears only willing to consider regulation of the transparency of online advertising. While this is an important area, it is less clear that Facebook and Google are willing to consider the need for regulations to combat issues like fake news or illegal content on their platforms.

Channel 4 believes policymakers must act now to ensure there is adequate regulation to protect consumers against harmful content through proper content standards by requiring platforms to remove illegal and harmful content. We note in particular the precedent set in Germany where a bill has been passed which will allow fines of up to €50m for social media firms which do not remove illegal content within 24 hours[623].

The digital giants are ostensibly publishers, who trade as media companies and therefore should be subject to the same regulations as broadcasters. The current regulatory system places much lower compliance burdens on non-broadcast operators, meaning less protection for the consumer. This imbalance should be redressed and there should be a "levelling up" of advertising codes to the highest level of protection available i.e. the UK Code of Broadcast Advertising.

Channel 4 acknowledges the positive industry initiatives to agree principles on key challenges faced by online advertising including around brand safety and ad fraud through JICWEBS but notes that neither Facebook nor Google are signatories thereby drastically limiting the impact and effectiveness of these initiatives. We concur with the conclusions of the Lords Communications Committee that *"industry should give these bodies greater powers to create and enforce rules establishing robust industry standards on measuring effectiveness and third party verification. If businesses fail to do so, the Government should propose legislation to regulate digital advertising"*[624]*.*

In order to ensure the scale and dominance of the digital advertising market is not supressing competition and reducing choice for consumers, Channel 4 believes there should be greater scrutiny of the size and dominance of these players in relation to the digital advertising market. This could include a review by the Competition and Markets Authority, for example.

[622] In 2017 Alphabet the parent company of Google /YouTube made $111bn in revenues and $13bn in profit whilst Facebook made $41bn in revenues and $16bn in profit

[623] https://www.theguardian.com/media/2017/jun/30/germany-approves-plans-to-fine-social-media-firms-up-to-50m

[624] House of Lords Select Committee on Communications UK advertising in a digital age https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/116/116.pdf

Channel 4 has also given particular thought to issue of Fake News and recommends a mix of measures to tackle the root causes driving the production as well as incentivising the provision of legitimate and trusted news content.

In particular, consideration should be given to the following options:

- **Kitemarking/prominence for regulated organisations –** Social media platforms should offer a system of kite-marking for UK news organisations signed up to a recognised system of external regulation such as Ofcom licensees, IPSO and IMPRESS. This would help the public identify legitimate news sources, particularly where fake news providers clone existing news sites or masquerade as false news providers. Social media platforms should also make kite-marked news providers more prominent in news feeds/search results to ensure that legitimate news sources are easily discoverable and not drowned out by fake news sites, and inversely make sure that fake news sites are not given prominence.

- **User feedback –** Platforms should be required to do more work to provide people with tools to differentiate between different types of content and to flag stories that have been reported by a critical mass of users as misleading or 'fake' news. Channel 4 recognises that ensuring that such user-led feedback does not impact on legitimate news stories is likely to prove logistically complex but it is important to ensure that stories that have been widely rebutted are flagged accordingly.

- **Industry-led solutions to restrict the incentives for fake news providers –** At present, the current practices and revenue agreements on social media platforms mean that the disseminators of fake news – as well as the online platforms - profit from clicks and views of fake news stories. Channel 4 notes that both Facebook and Google have updated their policies to restrict advertising around sites that publish misleading content but the effectiveness of these policies remains to be seen. Social media platforms must take greater responsibility of the ads that appear on their platforms and where they are placed. In addition, further work is also needed to protect the copyright of legitimate news providers on social media platforms. Other consumer brands also have a role in not supporting fake news sites by ensuring that they are not advertising around them.

- **Longer-term consideration of business models for journalism –** Consideration also needs to be given to the impact of digital platforms and fake news on business models for journalism in the longer term. If trusted news providers are to be the antidote to fake news, it is vital that they are able to monetise their content on these platforms and see a return on investment, particularly given the value that their content provides as both an important public good and as a content asset for social media platforms.

- **Measures to promote media literacy –** Ensuring that people have the tools to identify and critically assess news sources is crucial to tackling the impact of fake news. There is a role here for Ofcom, education institutions and PSBs to provide advice and guidance on how to verify and distinguish between verified and fake news sources. It is worth noting that YouGov research for Channel 4 found that almost half of adults (46%) think we need more fact checking sites – with significantly higher agreement among 18-24s (69%) and those that use Facebook as their primary source of news (60%). There is therefore also a role for news providers to build on existing work in providing fact-checking and verification services.

May 2018

Channel 4, BBC, and ITV – oral evidence (QQ 143-151)

Transcript to be found under BBC

Channel 4 – supplementary written evidence (IRN0117)

Answers to Select Committee on Communications: A Regulatory Framework for the Internet? Inquiry

TV-LIKE CONTENT

Question 9

What assessment have you made of the revision of the Audiovisual Media Services Directive insofar as it affects the regulation of TV-like content?

- Channel 4 believes the new AVMS Directive aims to achieve a better level-playing field in terms of regulation between linear and on-demand services. The revised AVMS Directive imposes more rules than the current Directive on VoD services, such as stronger obligations to protect minors, a 30% EU works quotas and some additional restrictions on alcohol advertising.

- Extension of Linear protection of minor rules to on Demand Services - Channel 4 believes this is in line with audience expectations that children need to be protected in a similar manner whilst watching the same content regardless if it is on linear or on-demand. Channel 4's All 4 service already abides by these rules.

- Advertising Minutage – Channel 4 opposed the EC's proposal for abolishing the hourly limit in favour of a daily limit. The revised text specifies that the daily limit of 20% applies from 6am to 6pm and that the prime-time window (where an additional 20% limit applies) goes from 6pm to 12pm. Channel 4 expects the UK to maintain its stricter current minutage rules.

- Extension of Scope to VSPs – Channel 4 welcomes the extension of the scope of the Directive to video-sharing platforms such as YouTube. This will mean VSPs will have to take measures to protect minors from harmful content and to protect citizens from hate speech, and will need to comply with rules that apply to audiovisual media services to protect consumers against inappropriate or subliminal advertising.

COPYRIGHT

Question 11

a) *Article 13 of the Copyright in the Digital Single Market Directive will place specific technological requirements for platforms. Is this the right model in your opinion?*

- Channel 4 did not take a position on Article 13 of the Copyright in the Digital Single Market Directive – the "value gap" provisions.

- Channel 4 agrees that sites such as YouTube and Facebook should take down content copyright infringement content pro-actively and expeditiously.

b) *Who should bear the costs of developing and managing these systems? The platforms or the copyright holders?*

- The big platforms such as YouTube and Facebook already use content recognition technologies. It would seem unfair that rightsholders would have to bear the costs for paying for filtering technologies as they suffer from copyright infringement of their content.

INTERNATIONAL REGULATION OF THE INTERNET

Question 12

a) *What are the risks if the UK introduces regulation without the co-operation of international partners, particularly the European Union?*

- This would depend on the policy measures. For example, any measures which may weaken data protection rules in the UK as agreed under GDPR or privacy on the internet would undermine the UK's ability to trade in data flows and services. This would undermine UK's leading position in e-Commerce and digital in Europe.
- Net Neutrality - despite pressure from some ISPs, the UK should continue to retain the EU's net neutrality provisions as the open internet has resulted in significant benefits for both consumers and businesses. Channel 4's All 4 is a beneficiary of the open internet provisions.

b) *What other international bodies should the UK work through to improve internet regulation?*

- Channel 4 welcomes Ofcom and Information Commissioner's office intentions to continue to co-operate with their EU partners post Brexit. Both organisations have played a prominent in sharing expertise and influencing EU policies.
- The UK should continue to work in international organisations such as the Council of Europe, OECD and the UN's Internet Governance Forum.

6 November 2018

Children’s Charities’ Coalition on Internet Safety – written evidence (IRN0008)

Is there a need to introduce specific regulation for the internet?

With the development of easy to use web browsers in the early to mid-1990s the internet started its journey from the confines of academia and limited adoption by business towards a mass consumer market. Unanticipated problems were not far behind. The increased availability of child sex abuse materials was one of them.

Questions about how or whether to regulate the internet first arose in public forums in the UK in 1996. This was the year Internet Watch Foundation was established.

At the time there was very little knowledge within Parliament, the Civil Service and the police about what the internet was and how it worked. Would this new-fangled technology take off or was it a passing craze? How much effort should be put into trying to understand it? There was therefore an almost palpable sigh of relief on the part of the Government when, after some difficult conversations, the industry agreed to “sort things out”. Thus, the IWF came into existence *faute de mieux.* It was not a carefully selected option, chosen from a range of available possibilities.

The internet industry then consisted principally of a handful of ISPs. There was opposition to the idea of forming the IWF but the majority view prevailed. Industry leaders were pleased to be left to their own devices. It married with a strong prevailing ideology among internet pioneers that, by building out the network, they were also building a new and better way of running the world.

John Perry Barlow’s “Declaration of the Independence of Cyberspace” spoke of *“Governments of the Industrial World, you weary giants of flesh and steel…..On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.”* This was an extreme exemplification, but it had resonances in many different virtual quarters.

Within industry circles there remains a strong attachment to self-regulation in everything that is connected to the internet. Undoubtedly this is rooted in part in an acknowledgement of the unique complexities presented by cyberspace, but it also picks up on, maybe exploits, a larger acceptance of the notion that smaller government is better government which, similarly, is connected with a diminution in confidence in public institutions generally.

However, the way events have unfurled since the mid-1990s, in particular the manifest failure of the internet value chain to find a way to reassure the public that the industry is both willing *and* able to find solutions to some of the problems that have developed, suggests the current arrangements for managing the internet in the UK are not working well enough.

Such internet regulation as exists in Britain today lacks coherence and consistency. It has grown up piecemeal, on an ad hoc basis not infrequently, as in the case of the IWF, following a crisis of some sort. As a result, we have a patchwork of powers and responsibilities distributed between different organizations, with varying degrees of transparency and apparent effectiveness.

On one count there are twelve different bodies[625] with a claim to being involved in regulating online activity. Moreover, there are limits to the extent to which these self-regulators, co-regulators and statutory regulators can or are willing to co-operate with each other.

Having twelve different organizations is not in itself the issue. However, our strongly held belief is someone somewhere should step back and take a view about what would be the *optimal* way to serve the public interest in this field. If the Select Committee cannot undertake this task perhaps it will be minded to recommend such an idea.

It may well be the case that in relation to certain types of activity self-regulation could continue to be the best possible answer to ensuring the public interest is properly safeguarded, but self-regulation has lost its historic right to be considered the default option. Henceforth, self-regulation should only be acceptable if it can be shown to adhere to processes and systems which allow members of the public to feel confident things are working to an agreed standard.

The lack of coherence and consistency in relation to internet regulation is by no means a peculiarly British problem. This does not mean the UK is powerless to act to protect or enhance its own best interests. Aside from anything else the value of the UK market to many online businesses means they will be unusually attentive to openly declared public policies and if they have the force of law behind them every significant online business will be keen to comply.

There will always be “tiddlers and rogues” who flourish around the edges or seek to exploit loopholes, but that ought not to deflect from mainstream concerns. It is possible to spend forever chasing the longtail when, by any reckoning and in accordance with the principles of proportionality, what the larger enterprises are doing is what matters to the vast majority of users. As smaller businesses grow so they will be drawn in. This may seem to be a little bit untidy, but the internet is untidy.

We have to start somewhere

It is a deeply entrenched myth in the liberal democracies that policies to address problems on the internet have to be internationally negotiated, agreed and implemented if anything lasting and worthwhile is to be achieved. This has the effect of paralysing Governments and legislatures and some companies, or lets them off the hook, providing an alibi for inaction. It serves to preserve, or at any rate prolong, the status quo. Cui bono?

[625] Ofcom, ICO, PSA, IWF, ASA, BBFC, CMA, DMA, GC, FCA, PRA, IPSO

Of course in some areas the greater the degree of international harmonization the more likely it is companies will voluntarily align (there are no certainties here, look at the story of IPv6) but equally it is true that in an environment where the ability to innovate is so highly prized, the role of leadership and rigorously thought through experimentation cannot be over-emphasised. If the UK develops an approach that is seen to be effective others will follow and eventually the "international community" will recognise and embrace it.

When BT first introduced "Cleanfeed" back in 2004, as a tool to restrict access to child sex abuse material on web sites, it did not consult the whole world before pressing ahead. It was criticised at the time by and in practically all parts of the internet, both here and abroad. BT nonetheless did what it thought was right and was technically feasible. "Cleanfeed" was seen to work. The practice is now widespread in all parts of the world and the idea behind it has even gained recognition within a 2011 EU Directive.

Similarly, when Prime Minister David Cameron announced the "We Protect" initiative in 2016 and arranged for £50 million to be put at its disposal he did not wait for the blessing or the opinion of the UN, the EU, ICANN, the IGF or anyone else. The Prime Minister did it and the current Government continues with it because they believed it was the right thing to do and would add value. The initiative is now widely recognised as ground-breaking.

When Microsoft developed and released PhotoDNA in 2009 they did so entirely of their own volition and it now ranks, globally, as one of the most significant advances in online child protection in recent years and it has been adapted to address other types of illegal content.

None of this is to minimise the importance of international institutions. On the contrary it is a matter of great regret that those that exist are not more energetically engaged in finding solutions to outstanding problems and some have a particularly lamentable history – here ICANN deserves a special mention. However, it is inevitable that geo-politics, diplomacy and the need to fund travel and find the time to attend international conferences are major limiting factors in terms of their speed and efficiency.

Children are not a small or marginal group

Whoever undertakes the sort of review we have in mind ought to be mindful of the fact that in the UK roughly 1 in 5 of all internet users is a child, that it to say someone under the age of 18. Globally, the proportion is 1 in 3, rising to nearly 1 in 2 in parts of the developing world. It is therefore the case that children are probably the largest single identifiable constituency of internet users, and even if that is not literally the case, they won't be far off.

Either way, there is no doubt that the internet is a medium for children every bit as much as it is a medium for anything else. This humdrum, ordinary fact is normally overlooked in the loftier climes of global internet policy making and by many individual internet businesses. Children are too often seen as an irritating, trivial concern, the responsibility of "someone else", usually parents, schools, the police, or all three, whereas our contention is that in any discussion about policy and the internet, in each and every forum, the fact that children are online in such gigantic numbers should be front and centre.

Two key US laws

One of the reasons children became marginalised as a factor in internet policy making circles can be traced back to two US laws.

s.230 of the **Communications Decency Act, 1996**, was the first legislative measure in the world to establish broad immunity from liability for intermediaries. The UK and the EU did not exactly copy it (eCommerce Directive) but they did not depart from it in a major way.

Recent changes in the law in the USA and in Europe have made some difference here but the core principle remains in place.

Immunity for intermediaries may have been critical in the early days of the internet, when there was a great deal of uncertainty about how the new technology would develop and there was justifiable concern about the prospect of law suits scaring off investors and slowing down innovation, but those days are long gone.

The internet is no longer a green field site. No one should be able to develop or market new products or services and plead ignorance in respect of well-known hazards. Yet the immunity laws are still in place. They have become a refuge for scoundrels.

The Children's Online Privacy Protection Act, 1998, introduced an incentive for companies to ban persons under the age of 13 from their services but the law did not create any obligation on businesses to enforce the age rule. No obligation meant zero incentive.

In the UK over 75% of all 10-12 year olds have accounts with social media platforms that specify 13 as their minimum age. In other countries the percentage is even higher. The social media companies could have chosen to police the perimeter. They didn't because they were not required so to do.

In effect this law and the immunity law combined to give online businesses permission to forget about children and many of them did. The GDPR will change the landscape but it is still too soon to say how.

What should be the legal liability of online platforms for the content that they host?

It would be unjust for any online platform to be held liable for any 3rd party content or behaviour where it did not have and could not have had any actual knowledge of it.

However, CHIS believes that in future, in order for a platform to maintain its immunity in respect of 3rd party content or behaviour, in either civil or criminal matters, it must show that, being mindful of available technologies, it had taken all reasonable and proportionate steps to prevent, limit or mitigate the scope for its service to be used for unlawful purposes AND that it has taken all reasonable and proportionate steps to ensure its stated terms and conditions are being honoured.

Terms and conditions of service which are not linked to any requirement to make good faith efforts to enforce them can be seen as being a pious hope, a marketing ploy or a deceptive practice. They convey the impression to a would-be user, or the parent of a would-be user, that certain things will or will not be happening or available on a site or service whereas in reality the service provider has no way of knowing if that is the case and they make no attempt to find out. That cannot be right.

How effective, fair and transparent are online platforms in moderating content that they host?

Online platforms vary enormously in their purpose, functionality and intended audience but CHIS cannot think of a single one where we could say we are confident their moderation policies are fair and effective, precisely because there is little or no transparency. Without an independent element which can verify that the statements a platform makes about its moderation practices are a true and fair reflection of what the company has actually done – rather as an auditor does with the commercial operations of a business – it will be impossible for us to take a different view.

What role should users play in establishing and maintaining online community standards for content and behaviour?

This sounds like a laudable democratic ambition, but our short answer is it depends on the nature of the platform and its functionality. If children are an intended audience or are in fact present in any appreciable numbers certain minimum standards should be applied and be enforced. Obviously consulting with users will always be a good and necessary part of sound business practice but the intention to consult or referring to the results of an apparent consultation should never be a reason for diluting, avoiding or delaying the adoption of acceptable minimum standards.

What effect will the United Kingdom leaving the European Union on the Government's regulation of the internet?

In the Max Schrems case the mighty USA was forced to change its laws in order to bring themselves into line with EU law. The alternative was US businesses would be barred from allowing EU customer data to cross its borders. We suspect the same will apply when/if we leave the EU. If we want UK businesses to continue being able to buy and sell things to people and businesses in the EU, if we want British young people to be able to communicate online with young people in other countries, our laws will have to correspond with the EU’s in several important respects. In this context the GDPR is likely to be the most relevant and since we are broadly pleased with GDPR from a child protection perspective, that is fine with us. It is obviously the case that, post-Brexit, the UK may have some greater latitude to develop new approaches and providing these do not collide with anything that matters to the EU this may work to the advantage of children in the UK. Time will tell.

27 April 2018

The Children’s Media Foundation (IRN0033)

Inquiry Response

1. The Children's Media Foundation is a not-for-profit organisation dedicated to ensuring UK kids have the best possible media choices, on all platforms and at all ages. We bring together academic research institutions, the children's media industries, regulators, politicians and concerned individuals who recognise that media is not only a powerful force in children's lives, but a valuable one.

2. This submission has been drafted by our non-exec advisory team, which comprises industry leaders from the children’s digital sector, researchers, and representatives from the tech-start up community. It is based on our knowledge of the children’s media industry, including audience research, and experience of developing best-practice products and policies for organisations in the UK and overseas.

3. The internet and digital media offer fantastic opportunities for children with respect to learning, entertainment and developing creativity. As an organisation we advocate innovation and high quality digital experiences available to children in an environment that is designed to be safe-by-default. Experience repeatedly demonstrates that is more effective to create universally safe spaces with specific areas that are restricted for more adult content, rather than the other way around.

4. The use of media by children is very different from adults. For a young child, YouTube is the preferred search engine rather than Google. Older children are instinctively disruptive. In the media space this is rarely borne out of rebellion, but rather a desire to overcome practical constraints such as cost of use (e.g. mobile data) and to discover new content. This means that the safety paradigms, such as walled gardens, that are proposed by adults are rarely effective in creating safe spaces for children.

5. A common argument is that apps provide safe spaces children. In many respects this is true, however it fails to address the challenge of discovery. With a billion apps in the app stores, it is almost impossible for children to discover new content and for brands to attract new users. That need is still being met by the web – and it’s the reason that all the major children’s brands maintain rich websites alongside apps.

6. Many of the recent controversies around internet safety – including the appearance of inappropriate content in the YouTube Kids app – have highlighted how social media platforms rely on technological solutions to address behavioural challenges. This is an approach that can never be 100% reliable, and consequently creates a digital landscape that is much more hazardous than ‘old’ media or even the real world.

7. Since its inception, many web users and digital businesses have

campaigned that the internet be maintained as a haven for freedom of expression that should not be regulated (https://en.wikipedia.org/wiki/Blue_Ribbon_Online_Free_Speech_Campaign). However, with freedom comes responsibility. The CMF has long argued that many web companies have shown complacency towards children – an argument recently echoed by the Health Secretary. As self-regulation has repeatedly fallen short, regretfully, formal regulation seems the best option to keep children safe online.

Questions

Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

8. Many of the standards and expectations surrounding the internet are derived from a time when it was a minority medium enjoyed (predominantly) by young men in Silicon Valley. That time is long gone: digital platforms are mainstream and media is ubiquitous in our lives.

9. With so many storms engulfing digital media over the last year, especially the social media platforms, it's evident that self-regulation is failing, and that a more robust framework of governance is required.

10. It's easy to conflate those controversies into a single problem. In reality they cover a variety of issues including:

    - Inappropriate material amidst children's content [626]
    - Data capture and privacy [627]
    - Editorial integrity [628]
    - Editorial standards [629]

11. In 'old' media, these issues are addressed through a variety of regulations enabled by legislation, and also a series of social contracts that have evolved between audiences and providers.

12. The CMF is concerned that as younger children have increasingly autonomous access to platforms and content, we must ensure that education for children and their parents at primary or even infant stages reflects these cultural changes. Research consistently demonstrates that digital media literacy is poor in many audience groups – including children and parents – and needs to be improved. But this cannot be the only solution. Digital media businesses also need to take more responsibility for their platforms and the content they provide.

[626] https://www.polygon.com/2017/12/8/16737556/youtube-kids-video-inappropriate-superhero-disney

[627] http://www.bbc.co.uk/news/topics/c81zyn0888lt/facebook-cambridge-analytica-data-scandal

[628] https://news.sky.com/story/sky-views-democracy-burns-as-facebook-lets-fake-news-thrive-10652711

[629] https://www.huffingtonpost.co.uk/entry/logan-paul-youtube-blasted-video_us_5a4b3372e4b06d1621ba4eb3

13. Rather than introduce new rules for new media, we would argue that the existing regulatory framework should be extended to include digital platforms available in the UK. However, the rules have to be enforced. The CMF considers that there are currently two main issues around regulation:

    a. Many major digital businesses popular with children fall outside UK jurisdiction.

    b. The wheels of technology move at a much faster rate than the cogs of the legal system. Legislation needs to be flexible to accommodate new challenges – and the industry needs to interpret the intention of guidance as well as the specifics.

14. Digital companies will often argue that regulation and control on the internet is too difficult. However, we would counter that if they can triangulate their user data to target content – and be confident enough to sell that as a service for advertisers – they should be able to understand if a user is a child. By contrast, the adult entertainment industry has been a strong advocate of age verification[630], and has developed and implanted technical solutions… Where there's a will there's a way!

What should the legal liability of online platforms be for the content that they host?

15. The liability of online platforms has often been a subject of debate in the courts and elsewhere. Google, for instance, has routinely argued that it is merely a facilitator allowing users to find[631] content. YouTube, Facebook and others have argued that they are merely platforms for distribution.

16. However, we consider that these arguments are no longer valid and must be reconsidered.
    Companies such as Facebook[632], Amazon[633] and YouTube[634] are commissioning original content for their platforms and using this content to drive revenue. Whether by accident or design, search engine algorithms are the de-facto curators for most people's access to content online. The platforms are using this curation to drive their revenues.

17. In many respects these business models are no different from those of old media - newspapers, film and TV. We therefore dispute that online platforms are merely distributors and contend that by default they should be considered as publishers.

[630] https://www.dpalliance.org.uk/groups/age-verification/

[631] e.g. https://www.lawgazette.co.uk/law/media-is-google-a-publisher-or-merely-a-facilitator/52408.article

[632] http://variety.com/2017/digital/news/facebook-last-state-standing-1202464126/

[633] https://en.wikipedia.org/wiki/List_of_original_programs_distributed_by_Amazon

[634] https://en.wikipedia.org/wiki/YouTube_Original_Channel_Initiative

What role should users play in establishing and maintaining online community standards for content and behaviour?

18. Users should take some responsibility for maintaining community standards. However accountability needs to reside with the platforms themselves. This is particularly important for communities used by children.

19. The CMF considers that any platform widely used by children, whether intended for them or targeted at them or not, should have an accessible, clear children's policy.

20. Children's TV presenter Ed Petrie recently highlighted the gulf in editorial standards between a traditional channel such as CBBC (reach, approx. 1.5 million/week[635]) and YouTube's Logan Paul (15 million mostly young subscribers).

21. While Logan Paul is often portrayed as a free-thinking vlogger, he is an example of a YouTuber who has been supported and promoted by the platform itself. On that basis it is difficult to argue that the platform is not accountable for the challenging material he posts.

22. The CMF believes that platforms such as YouTube, that are based on user-generated content, should contribute to the training of their high-profile users and maintain clear editorial policies.

23. Repeated studies show that children are heavy users of social media[636], however the major social platforms consistently refuse to take responsibility for younger users. WhatsApp, for instance is about to change their terms and conditions to preclude under-16s – even though a third of 12-15 years olds in the UK are thought to have accounts. The likelihood is that few of these users will delete their accounts, so they will continue to use WhatsApp in breach of the T&Cs. While companies such as WhatsApp are operating perfectly legally, we do not feel it is right that the onus is placed entirely in the hands of children and parents. The platforms must assume some responsibility.

24. We advocate the development of a universal set of guidelines, derived from best practice, that is should be owned by a governance-body and adopted by the digital. This is a model that has worked well to safeguard the rights of children in other sectors - such as the watershed in broadcasting[637] and harassment by the press[638] and banning alcohol ads that could be appealing to children[639].

[635] https://downloads.bbc.co.uk/aboutthebbc/reports/pdf/audience_0711.pdf

[636] e.g. https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-parents-2017

[637] https://www.ofcom.org.uk/tv-radio-and-on-demand/broadcast-codes/broadcast-code

[638] https://www.ipso.co.uk/editors-code-of-practice/

[639] https://www.asa.org.uk/codes-and-rulings/advertising-codes.html

What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

25. Freedom of expression and freedom of information are obviously vital tenets of British society. While the CMF seeks to improve the safeguards and rights of children online, we would not advocate any form of outright censorship.

26. The free, self-publishing nature of the internet means that it is often heralded as a bastion of free speech and expression. However, this is far from today's reality. While self-publishing is straightforward, making that content discoverable is much harder. This is achieved through search engines and algorithms developed for commercial purposes. As the US election has illustrated[640], this means that what constitutes freedom of speech is actually defined by a few large commercial organisations rather than the society in which they operate.

27. From a children's perspective, the recent problems concerning YouTube Kids highlight the concerns the CMF has about placing too much trust in algorithms. However, we do recognise the commercial need to keep the detail of algorithms confidential.

28. While we would not expect companies to reveal their algorithms, we would like to see some accountability via the publication of the editorial guidelines and values that underpin them.

What information should online platforms provide to users about the use of their personal data?

29. The collection and exploitation of user data is an on-going concern. The implications for children are even more significant, as they may not understand the long-term implications of sharing data, or have the capacity to make informed decisions. The GDPR will improve the visibility of data protection. However, in reality many of the principles of the GDPR are already reflected in the 1998 Data Protection Act - which means that data controllers should already tell their users about the data they hold.

30. The Internet of Things poses new risks. As more and more devices become 'connected', and more and more businesses collect data, there is the potential for data protection standards to degrade as a result of hacks, mishaps or simple complacency. If this were to happen, it could have important implications for children as well as adults.

31. Our concern is that the terms, conditions and instructions on accessing or providing data are often presented discretely, and in terms that are impenetrable for most people – especially children.

[640] https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory

In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

32. As outlined above, while we would not expect companies to reveal their algorithms, we would like to see some accountability via the publication of the editorial guidelines and the values that underpin them.

What is the impact of the dominance of a small number of online platforms in certain online markets?

33. From both an industry and audience perspective the dominance of a few platforms is distorting the entire media market.

34. The British children's media industry, including many supporters of the CMF, has an international reputation for high quality content. Historically this has been driven by a few UK broadcasters commissioning innovative and challenging programmes, some of which have achieved international success.

35. There is a common assumption that new media will offer new revenue models for content makers. However producers tell us that the market is extremely unbalanced. While a handful of original digital commissions are extremely well funded, notably by Netflix or Amazon, few of these are currently commissioned in the UK. On platforms such as YouTube content generates revenue through advertising. But whereas a children's show on a TV channel might cost anything from £50,000 to £300,000 per hour, a video on YouTube will earn only around £1,000 for a million views. This is not an income that can fund the development and production of high quality content.

36. From a user perspective there are similar challenges. There can be no doubt that YouTube is a hugely popular platform, well used by audiences, including children, and carrying some outstanding content. However the challenges of curation and discovery make it hard for children to find new, culturally relevant content by serendipity – as they did in the past on television channels. The most popular videos for children on YouTube are US originated animation, or low quality videos designed to provide 'playground currency' – e.g. "unboxing videos". In the case of YouTube the dominance of the platform means there is no alternative.

37. We are also concerned that the dominance of these platforms is suppressing the development of innovative experiences online. On YouTube itself the choices are endless, but algorithmic recommendation refines this down to the more popular content and "more of the same". This compounds the common concern amongst parents that algorithmic curation is a poor moderator of content that is inappropriate for children.

What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

38. In the media industry, European legislation is recognised as being best-in-class in terms of respecting and safeguarding the rights of children. We welcome the government's commitment to GDPR post Brexit.

39. However, data and privacy are not the only issues. The CMF is also mindful of issues such as the commercialisation of content, and the need to reflect the lives and needs of British children in digital media.

40. While we may expect some European countries such as France to strictly legislate, the UK's tendency is to let the market self-regulate. So far this has not been successful. We are concerned that the government's stance on this may not substantially change.

41. We contend that UK regulators need to have 'teeth' to ensure that regulation can be enforced. As a smaller, autonomous market post-Brexit, the risk is that the UK's influence on the major digital businesses will wane.

42. The internet is designed to be distributed and not limited by national borders. Therefore we need to ensure that regulation is developed collaboratively with other countries.

43. However, it is also important to ensure that the lives and culture of British children are reflected in the media they consume and, if that media is to be substantially on social media and video-on-demand platforms, then consideration needs to be given within regulatory frameworks to content quotas or incentive schemes to encourage continued support for home-grown talent and creativity. Equally innovation and challenging, relevant content need to be stimulated. In that respect, we hope that the EU's policy[641] to require a percentage of streaming content to be produced locally, will be adopted by the UK post Brexit.

11 May 2018

[641] https://ec.europa.eu/digital-single-market/en/news/proposal-updated-audiovisual-media-services-directive

The Children's Society and YoungMinds – written evidence (IRN0025)

About YoungMinds
We exist so that young people have the strongest possible voice in improving their mental health. We strive to make sure everything, from Government policy to practice in schools and services, is driven by young people's experiences and aspirations.
We support parents to help their children through difficult times, we equip professionals to provide the best possible support to the young people that they work with, and we empower young people to change their world.

About The Children's Society
The Children's Society is a leading charity committed to improving the lives of thousands of children and young people every year. We work across the country with the most disadvantaged children through our specialist services. Our direct work with vulnerable young people supports missing children, children with experiences of sexual exploitation, children in or leaving care, refugee, migrant and trafficked children. We can place their voices at the centre of our work.

Introduction

We welcome this Inquiry from the Committee into improving internet regulation. The internet has become an increasingly significant part of young people's lives, with the amount of time they spend online a week more than doubling from 2005 to 2015.[642] We know that a lot of this online use is on social media sites - our joint inquiry into cyberbullying found that nearly half (44%) of children and young people spend more than three hours per day on social media.[643] There are growing concerns around the impact of social media use on children and young people's mental health and well-being, and how social media companies are responding to online risks such as cyberbullying.

The Children's Society and YoungMinds have recently carried out a comprehensive inquiry, in collaboration with Alex Chalk MP, into the impact of cyberbullying on social media on children and young people's mental health. The inquiry also looked at what social media companies are doing to both prevent and tackle this problem.

This is a joint submission from The Children's Society and YoungMinds. It will give a brief overview of the inquiry's key findings and recommendations. A full version of the report can be accessed here.

1. Scope of the inquiry

[642] Przybylski, A. K. and Nash, V. Internet filtering technology and adversive online experiences in adolescence The Journal of Pediatrics (184) 215 – 219. Available: http://www.jpeds.com/article/S0022-3476(17)30173-7/pdf

[643] https://www.childrenssociety.org.uk/sites/default/files/social-media-cyberbullying-inquiry-full-report_0.pdf

Our inquiry into the impact of cyberbullying on children's mental health was led by Alex Chalk MP, with the support of a cross-party panel of MP's and internet safety experts.

The inquiry sought to examine:

- Children and young people's experiences of bullying on social media platforms and how these experiences have affected their well-being;
- The effectiveness of existing interventions to protect children and young people from bullying on social media platforms;
- The effectiveness of social media companies existing approaches to preventing and responding to cyberbullying and how they might be strengthened.

The evidence presented in the inquiry is based on a combination of survey views of children and young people; oral evidence from children and young people and experts; a review of academic literature; and insight from organisations and institutions with an interest in children and young people's experiences of bullying online, mental health and internet safety. We also took evidence from major social media companies.

2. Key Findings from our inquiry

2.1 The scale of cyberbullying

Social media has exacerbated the occurrence of online bullying. As part of our inquiry, over a third (39%) of young people told us they have experienced cyberbullying in their lifetime and 15% reported being bullied online in the last month.[644] The more time children and young people spend online, the more they reported having experienced cyberbullying in the last year – more than half of those who have experienced online bullying spent more than three hours a day on social media.

Young people said that, due to experiencing cyberbullying, they are more concerned by what content was being posted online about them, and consequently would monitor social media more frequently. The continuous checking of social media can heighten underlying anxieties, lowering self-esteem, or even creating addictive/obsessive beliefs and behaviours.

There are well-established links between bullying and low well-being – The Children's Society's well-being research has consistently found that children who have been bullied are much more likely to have low subjective well-being than other children. What is more, when looking at the specific impact of cyberbullying on well-being, research from the University of Birmingham found that children and young people who have experienced cyberbullying are more

[644] https://www.childrenssociety.org.uk/sites/default/files/social-media-cyberbullying-inquiry-full-report_0.pdf

than twice as likely to self-harm and attempt suicide than those who haven't experienced online bullying.[645]

2.2 Age appropriate content on social media platforms

The minimum age requirement for most social media companies is currently set at 13 years old. However, results from our survey of children and young people found 61% of children first created their social media account before the prescribed age limit of 13.[646] Ofcom's annual survey also found that by age 12, half of all children have a social media profile.[647] This means that many children below the age limit who are using social media may be at greater risk of online harm as these platforms are not designed with their usage in mind.

The inquiry heard from expert witnesses on how social media companies do not do enough to identify those under the age of 13 using their platforms. One witness told us that '*social media companies are not proactive about this because customer need is a priority in relation to functionality.'* It's important that social media platforms establish age-appropriate design and communication for children to reflect the reality of under-13s using these platforms.

What is more, young people told us they do not always read the Terms and Conditions on social media platforms, and therefore do not fully understand their rights or the safeguards in place to protect them. Evidence heard in the inquiry stated that social media companies do not go far enough in communicating rights and expectations in a clear enough way, with one witness noting, '*Terms and conditions are not usable for young people. They do not read them and so are not understanding their rights…Young people must be involved in this process.'*

Recommendations:

- *Social media platforms must be age-appropriate, and companies should pilot approaches to identify under-13's and gain explicit parent consent.*
- *The Government should put children's experiences at the heart of internet safety policy development.*
- *Social media companies need to ensure that children and young people understand their rights and responsibilities when using their platforms.*

2.3 The role of social media companies

Whilst social media companies have gone some way in educating children about their platforms and online harms, there is still more that can be done. The inquiry heard from social media companies who did accept the responsibility they have to ensure users use their platforms safely but noted there is no shared understanding and approach to this.

[645] The University of Birmingham. 2017. Young victims of cyberbullying twice as likely to attempt suicide and self-harm. Available: http://www.birmingham.ac.uk/news/latest/2017/08/young-victims-cyberbullying-suicide.aspx

[646] https://www.childrenssociety.org.uk/sites/default/files/social-media-cyberbullying-inquiry-full-report_0.pdf

[647] Ofcom. 2017. Children and Parents: Media Use and Attitudes Report. Available: https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parentsmedia-use-attitudes-2017.pdf

The inquiry highlighted that whilst the duty to protect children online is relevant to both small and large social media companies, the lack of attention given to the operation of start-up companies potentially drives young people to these less regulated platforms and is placing them at greater risk. One witness noted:

'There is a risk that by driving young people away from the big companies such as Facebook through negative headlines, they may go to less moderated sites and those anonymous apps that cause greater problems and lack of traceability.'

Children and young people consistently told us in the inquiry that the response they receive from social media companies following a report of cyberbullying is slow and inadequate. The overwhelming majority of young people (83%) think social media companies should be doing more to tackle cyberbullying on their sites.[648] Young people also generally reported that they felt the onus is on them to deal with the cyberbullying, and that those who engage in cyberbullying face no consequences for their actions.

2.3.1 A lack of transparency and accountability

There is a lack of accountability about how effectively social media companies respond to reports of inappropriate content, bullying or other risks. To date, social media companies have largely been operating in ungoverned digital landscape through a system of self-regulation. Whilst the Government's Internet Safety Strategy recognises the need for online providers to play a greater role in protecting children and young people from online harm (including cyberbullying), there is currently no legal or regulatory framework in the UK that places a duty on social media companies to safeguard children from cyberbullying.

There is also a need for greater transparency from social media companies as they do not consistently record and report on the nature, volume and outcomes of complaints made within their systems. This makes it challenging to assess the success rate of social media platforms in tackling cyberbullying and other online risks.

What is more, throughout the inquiry we repeatedly heard that there was poor information and transparency about social media companies moderation processes – including details about the number of moderators, how decisions are made, their training and the tools available to them. Young people also noted a lack of transparency about reporting cyberbullying, not knowing when they would hear back or about the progress of their report.

2.3.2 Education on online risks

Social media companies are in a unique position to be able to educate young people and their parents about online safety. In recent years, large social media companies have taken steps to launch and invest a range of initiatives aimed at raising awareness of online safety. For example, YouTube runs a programme to

[648] https://www.childrenssociety.org.uk/sites/default/files/social-media-cyberbullying-inquiry-full-report_0.pdf

help young people spot the signs and understand inappropriate behaviours on its platform, and Facebook and Instagram have resource hubs to support young people and provide the signposting information they need.

Young people told us that companies should play a key role in educating young users and their parents about the risks faced online. They felt that social media companies should look at how they can incorporate an educational element alongside restrictions to ensure that those who breach their guidelines learn from their mistakes.

Recommendations:

- *Social media companies should provide timely, effective and consistent responses to online bullying;*
- *The Government should improve accountability by requiring social media companies to publish data about their response to reports of online bullying;*
- *The Government should teach children and young people to be safe and responsible online, and ensure they know how to respond positively to online harms such as cyberbullying.*

3. Summary and recommendations

Evidence received into our inquiry was clear that social media companies need to do more than they are currently to prevent and respond effectively to online bullying and harm. We have identified a number of issues that need to be addressed to ensure that social media companies together with the Government, schools, families and industry play their part in creating a safe digital environment.

Recommendations:

- *Social media platforms must be age-appropriate, and companies should pilot approaches to identify under-13s and gain explicit parental consent;*
- *Social media companies should enable children and young people to understand their rights and responsibilities when using social media;*
- *Social media companies should provide timely, effective and consistent responses to online bullying;*
- *Social media companies should prioritise the promotion of children and young people’s mental health and well-being across their platforms;*
- *The Government should improve accountability by requiring social media companies to publish data about their response to reports of online bullying;*
- *The Government should commission additional research into the scale of online bullying, and its impact on children and young people;*
- *The Government should put children’s experiences at the heart of internet safety policy development;*
- *The Government should teach children and young people to be safe and responsible online, and ensure they know how to respond positively to online harms such as cyberbullying.*

11 May 2018

Cloudflare – written evidence (IRN0064)

Cloudflare[649] appreciates the opportunity to respond to the House of Lords inquiry/call for evidence on the question of *The Internet: To Regulate or not to Regulate?* As the internet and business models continue to evolve, it is important that policy makers take stock at regular intervals, to examine the continued validity of existing governance models and any impacts on end users.

It is critical that an evidence-based approach is taken during any policy development process and that there is a precise problem definition. We submit this contribution in the hope that it may enrich the debate.

A Nuanced Approach to Internet Governance and Regulation

In the main, Cloudflare is a cybersecurity and web acceleration company, operating deep within the internet stack. Our expertise is in moving internet traffic around the globe quickly and securely, and protecting against the threat of cyber-attacks. Cloudflare's business is not about analyzing the content that flows over its network but is rather about securing and optimizing the process used to get the content to where it needs to go. As such, Cloudflare's services form part of the public core of the Internet, sitting at the infrastructure level, and they facilitate the business of other providers, such as those at the application level.

The Internet is a complex ecosystem made up of many different layers, players and business models. Therefore, references to regulating "the internet" are much too broad stroke, and a more nuanced approach should be taken, attributing different roles and responsibilities according to different layers and actors within the internet stack. For example, the roles and responsibilities of infrastructure providers are very different to consumer-facing platforms which manipulate and organise content.

The public core of the internet has been a particular success story of the internet eco-system. In general, costs are declining within the industry due to scale, and end users are the beneficiaries. Quality and efficiencies are constantly on the rise, industry peering works well and network investment is ongoing. Cloudflare continually seeks out ways to upgrade and expand its network and provides a global Content Delivery Network (CDN) service with unique performance optimization capabilities: we cache static content, accelerate dynamic content, and make it easy to optimize outbound content. We operate a massive, horizontally scaled architecture in which every node can perform DNS requests, security checks, and performance transformations. The combination of this architecture and network produces a reliable, high-performance service for end users, and all this has happened in the absence of internet regulation.

A question to be asked when considering the layers within the internet stack that could be suitable for some form of regulation is whether any action that an internet company might take is visible to and/or expected by internet users, and whether such users have a direct relationship with the company. To illustrate

[649] https://www.cloudflare.com/

this point, while 10% of all web requests worldwide flow through the Cloudflare network, the vast majority of users are not aware that they are touching the Cloudflare network at some point.

Existing Internet Regulations and Norms

It is not correct to say that the internet is not currently subject to regulation. Indeed, there is a variety of rules and laws applicable to the online world, such as those around data protection and privacy, consumer protection, security and copyright. These are complemented by norms in cyberspace, such as transparency, openness and due process, and principles set out in agreements such as the European Convention on Human Rights and the European Charter of Fundamental Rights. It can also be said that the multi-stakeholder, bottom-up approach to governing the internet had seen great success, as demonstrated by the work of bodies such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Engineering Taskforce (IETF).

The EU eCommerce Directive and the intermediary liability regime has been a pivotal piece of legislation which has enabled the internet ecosystem and innovation to flourish. We believe that the liability principles remain sound to this day, in particular the manner in which the framework addresses specific activities (eg hosting, caching) rather than companies or particular business models. It would be a major concern for business - particularly those businesses operating across borders, which is almost a given in the internet industry - if the U.K. was to depart from this well-established regime since legal certainty and continuity is a key component for ongoing investment.

Ensuring Continued and Inclusive Innovation

While there may be some issues arising as a result of the behaviour of large and dominant internet platforms, it should not be forgotten that many small and medium-sized companies also benefit from the protections of the intermediary liability regime and these enable SMEs to offer their services and gain a foothold in the market. As such, targeted initiatives - including of a self-regulatory nature - may be more appropriate to address any issues or perceived harms, and the scope of such measures should be clearly defined so as ensure that “the internet” at large and, importantly, the well-functioning infrastructure layer, is not caught in unnecessary cross-fire.

We remain available for any follow-up and further questions.

May 2018

Coalition for a Digital Economy (Coadec) and techUK – oral evidence (QQ 44-51)

Tuesday 22 May 2018

Watch the meeting

Members present: Lord Gilbert of Panteg (Chairman), Lord Allen of Kensington; Baroness Bonham-Carter of Yarnbury; The Lord Bishop of Chelmsford; Lord Goodlad; Lord Gordon of Strathblane; Baroness Kidron; Baroness McIntosh of Hudnall; Baroness Quin.

Evidence Session No. 6 Heard in Public Questions 44 - 51

Examination of witnesses

Dom Hallas, Executive Director, Coalition for a Digital Economy (Coadec); Antony Walker, Deputy Chief Executive, techUK.

Q44 **The Chairman:** Can I welcome our witnesses to this session of the Communications Committee inquiry on internet regulation? Our first witnesses are from the Coalition for a Digital Economy and from techUK. You are very welcome.

Today's session is broadcast online and a transcript will be taken. We will not be voting today, so we will have an uninterrupted session. Perhaps I can ask you to introduce yourselves and tell us about your organisations. What are your thoughts on the economic impact of online regulation, the impact on start-ups and innovation, and the likelihood of big tech companies to locate in the UK if we get regulation wrong or overregulate?

Dom Hallas: Thank you very much for having us here. I am the executive director of the Coalition for a Digital Economy, or Coadec for short. We represent start-up and scale-up technology businesses in the UK to Parliament and other political stakeholders. There are over 220,000 digital businesses now in the UK on the latest figures. The vast majority of those are not the tech giants you see every day in the news. In fact, they are the traditional SMEs or, as we call them, start-ups and scale-ups that drive the British economy.

When Coadec was founded in 2010, it was a real outsider voice and at the edges of the political debate. Reflecting the shift and the role of tech start-ups and scale-ups in the UK economy more broadly, we have moved closer and closer to the centre to the extent that I now sit on the Digital Economy Council with the managing directors of Facebook and Google for the Government and have engaged extensively throughout Whitehall and Westminster on those issues, as well in Brussels.

I have worked on tech policy for the bulk of my career, including the dark days of the GDPR, for those us who have been involved in it, including Antony. Until January, I worked at the Department for Exiting the European Union on diplomatic strategy until I took over in January as the executive director of Coadec.

To answer your question about economic impact, as I said, the role that start-ups and scale-ups have played in the British economy has been vast. We have seen that development has been absolutely extraordinary. We are talking about 30% in the past five years of additional technology value in start-ups and scale-ups. There are now 800,000 programmers in the UK. Some 300,000 of those are in London, but half a million of those are outside of London. That is the important issue here. A lot of the perception of technology is that it is quite an elitist institution and we are talking about hipsters in Shoreditch. The reality is that these days that is absolutely not the case. It is a much broader and more important part of the economy. Regulation and the stability of that legal framework in the United Kingdom has been critical in allowing those start-ups to develop.

Antony Walker: I am deputy CEO of techUK, a technology trade association representing approximately 950 companies that operate here in the UK in digital technology companies. That includes the very largest global companies all the way through to a long tail of medium-sized and smaller UK firms. We represent the breadth of very large to small.

To answer your question on the economic impact of regulation, regulation can have a very positive economic impact. Good regulation can be enabling. It provides a clear framework in which businesses can operate and do business on a basis of trust between each other and on a basis of trust with their consumers. When we get it right, good regulation can be extremely positive. Indeed, I would argue over the last 20 to 25 years, we have seen a process of progressive development of regulation that relates to the online economy.

We do not recognise the depiction of the internet as a kind of wild west. There is a huge amount of law that has been developed specifically for the digital world. Of course, there is lots of common law that applies directly to online and offline. As long as we make sure that it is proportionate, targeted, focused on clear outcomes and that it delivers against those outcomes, it can be very positive.

In terms of the economic opportunity for the UK as we enter the next phase of the digital economy, if we can continue to get the policy and regulatory environment right for businesses, that will attract investment to the UK. All that is predicated on getting it right and getting into the detail of understanding the implications and understanding what works and what does not work, which I am sure we will get into in the course of this discussion.

The Chairman: In the course of our inquiry, some witnesses have advocated the Australian system of online regulation in which it is argued that a tiered system of regulation with greater burdens on the larger tech companies and reduced burdens on start-ups and innovative companies is the way forward. Have you studied the Australian regulatory system? Do you have any observations on it?

Dom Hallas: I would not necessarily describe it as a tiered system. The Australian system is more about dividing into good actors and bad actors. My understanding is that if you do not opt into the system, you are put into the higher camp. That is not necessarily about size.

More broadly, talking about tiered systems, there is a challenge that is ultimately that all start-up businesses want to grow. The idea of restricting the goal of innovation by constantly placing additional regulatory requirements on them when they may not be necessary is a challenge. Something we are seeing from the European Union at the moment is a conversation about looking at what the biggest tech giants can do—the Googles and Facebooks—and thinking about scaling that down to smaller companies. This is a mistake and misunderstands the nature of the way in which regulatory compliance and those functions would grow within a business.

The other thing about the Australian system, and I know that the Irish Government were also looking at this, is that it is incredibly expensive to administer for the outcomes we are talking about. About 700 complaints about cyberbullying have been filed with the Government over the past three years under the Australian system. The system costs about £15 million. That is Cones Hotline-esque value for money. I would not necessarily advise that. I know that the Irish Government have looked elsewhere for options.

Antony Walker: First of all, the scope of this example is focused on one particular issue of cyberbullying. It is a very specific issue. As my colleague said, you can argue about whether the apparatus that has been put in place is proportionate to the particular challenge or whether it is the right way to get to the challenge.

To answer the broader question of whether the same rules should apply for large businesses and very large platforms versus new entrants, one thing you do not want to do is create regulation and legislation that entrenches incumbency. You do not want to make it hard for new companies to come in and new platforms to emerge that can challenge the established platforms. An unintended consequence of regulation is that, if you are not careful, you can do that by making the regulation a significant barrier to entry.

Clearly, we have to recognise that small companies will want to scale and grow quite quickly, so it is good to get them thinking about the implications of their services as they grow in scale. You want them to be pointing in the right direction when they are constructing their services and thinking about the risk for unintended harm. The Australian example is interesting, but I am not sure it tells us a lot about what we should be doing here in the UK.

Q45 **Baroness Kidron:** Before we get to the question of regulation, are there design features inherent in the common services that worry you? I am thinking about things such as echo chambers, compulsive technologies, and maybe some of the things that we are looking at with regard to the internet of things and smart toys. Take your pick.

I am interested to know whether either or both of you have some concerns niggling at the back of your mind about what is out there and how it might affect users.

Dom Hallas: These are important issues that everyone is now debating, including us. I am a technology evangelist, which is why I do the job that I do. It is a very good thing for society and will continue to be.

On issues such as addiction to technology and the way these services are designed, we have heard all this before. I was not around in the 1970s, but I am reliably informed by my mum that there was a big discussion around people being addicted to television. Certainly, in my era there was a big conversation around the impact of things like video games. It is important to set any discussion about the newest coolest technology and the impact that it will have in the broader context of the gradual development of different things.

Baroness Kidron: There is nothing that worries you as it stands.

Dom Hallas: It is important to debate these issues as a society. Personally, nothing particularly worries me. Ultimately, "you are the law makers here", is what I would say.

Baroness Kidron: Indeed.

Antony Walker: There are lots of digital technology platforms that have developed incredibly quickly and have scaled incredibly quickly. When you have services like this that are used by so many people on a daily basis, you start to see behaviours and consequences that were not always easy to predict at the outset and that you may determine have consequences that need to be explored.

We are clearly in that phase of starting to understand some of the implications of the very wide use of social media and other technology platforms. We are starting to see things that we think are great and are positive. We are also starting to wonder about the implications of the sort of behaviour that we are starting to see and whether the design of that service is driving towards a behaviour or an outcome that is less desirable.

There are issues that are of concern. They are mostly out there in the public debate. At the moment, we are having a very lively debate about some of the implications of living in a digital world. In the technology sector, I have seen a lot of people, particularly technologists looking at the next generation of technologies and artificial intelligence, who absolutely recognise that we need to be extremely thoughtful about how we develop the next generation of technologies, particularly when we have seen some of the outcomes from the current range of technology—hence the big focus on digital ethics and the very live discussion that is taking place internationally on the choices that technologists, researchers and businesses make when it comes to the application of new technologies.

So, yes, I would say there are issues that are of concern. The question is how to address them.

Baroness Kidron: Funnily enough, that was my follow-up question. Thank you for getting there so swiftly. Where does that responsibility lie? Mr Hallas has already said, "That's for society to discuss". In a way, regulation is an expression of society's view about what is acceptable or not acceptable. Is it now time for us to be thinking about the design rather than the content, which has rather preoccupied everybody and is possibly of less import, frankly, than the design and structure of services?

Antony Walker: There is increasingly a discussion about design. Within GDPR, you have the principle of privacy by design. Concerns about cybersecurity are leading to a big focus on security by design. They are two situations where we are very clear about the desired outcome and what harm we are trying to mitigate. In areas such as echo chambers and hate speech, the norms are less clear. That is why the design part is more difficult. You are trying to get companies and people developing technology to anticipate issues that it may be for society to debate what the desired outcome could be.

Do I think design is important? Yes. Do I think we need to be very careful, particularly when we think about AI, to think through the implications of where we are applying AI and to what purpose? Absolutely. We should also recognise that these are complicated issues. It will not always be clear exactly what the right and wrong thing to do is.

Dom Hallas: Building on that, this conversation about outcomes is absolutely the right one to be having. We understand that these issues are complex. At a societal level, it is important to debate and discuss what we want those outcomes to be. This is the case for the GDPR. It is also encouraging to see this built into the Government's *Internet Safety Strategy* Green Paper response that came out over the weekend. It is sensible to have the conversation with industry, the start-ups and scale-ups and all the technologists about how to implement that to deliver those outcomes as opposed to the line-by-line regulation that can be quite burdensome and have that economic impact that we are concerned about.

Baroness Kidron: If I might quote you back at yourself, would you not recognise that society might put value on spending $15 million to save 700 bullied children and companies will not? There is a balance that society has to dictate as well as be informed by the need.

Dom Hallas: I do not necessarily speak for those companies, but the vast majority of companies have processes in place, which can be criticised. Society has a right to ask them to do more. My broader point was that replicating something that could be delivered effectively through guidelines and the encouragement of industry to do certain things.

Baroness Kidron: We look forward to industry doing those things.

Antony Walker: Can I make a comment on the bullying issue?

Baroness Kidron: I am sorry. I was not making a narrow point about bullying; I was talking about values rather more broadly.

The Lord Bishop of Chelmsford: Mr Hallas, you described yourself as an evangelist.

Dom Hallas: Which you are quite aware of, yes.

The Lord Bishop of Chelmsford: It is a subject that I know a little about. In my experience, the best evangelists are those who can acknowledge the weaknesses and challenges in their own arguments. I am also probably about the same age as your mother. I have to say, and I say it with a smile, that your answer sounded very complacent. The issues that we are facing as a society now over addictions, particularly among children and young people, are of a completely different order.

You are right that there were concerns about television and video games, but it was much easier to exercise control over those in society, particularly in the family. It is much harder in the world we are now inhabiting. You are on the record in this conversation. I wondered whether you wanted to rethink your answer. Surely you can see that there are some issues here to do with addictions. You sounded as though you were saying that there is no problem—"It is in people's imagination. We had this in the past and that's the end of it".

Dom Hallas: I do not think that is necessarily what I was saying.

The Lord Bishop of Chelmsford: That is what we heard.

Dom Hallas: In which case I should restate my case. As a society, we think about what we want from companies, and that is the role that you play as law makers. When I was talking about the past, as in those discussions, I am not saying that legitimate points are not being made on both sides. As you say, you know a lot more about the definition of an evangelist than I do. There are a lot of people with a more negative view of technology in the world right now. The important role that I play as executive director of Coadec is to put across the point about the economic value and the broader social good.

The Lord Bishop of Chelmsford: What I am putting to you is we are more likely to take your evidence seriously if you acknowledge that there are some real issues here that we need to address together and find solutions to together.

Dom Hallas: I am here to talk on behalf of e-commerce businesses, for example, one of which I met last week in Leeds. It makes greeting cards. The important thing is that we do not lose sight of the idea that the broader digital economy is much broader than the issues that we are talking about, as important as those issues might be.

Baroness Kidron: Both of you seem to suggest that it is a question of striking the right balance. Is the balance right at the moment? What worries me quite a lot is the fact that users, to get the information they want, share a lot of information about themselves in that process. Obviously that is in companies' interests, because they target those people with adverts and information which they think they might be interested in. It can be seen by the user as something of an invasion of privacy. Is the balance right at the moment? Does the balance need to be changed?

Antony Walker: This is a central issue. For anybody who is busily deleting GDPR emails, we recognise that there is a major change in the law coming though, which has proved to be very timely.

On the issue of privacy and the relationship between data subjects, like all of us, and other organisations, we are going through a moment rebalancing. We will see what the implications of that will be. The GDPR was debated in enormous detail in the European Union, in this House and elsewhere. That whole process was about striking a balance. We are going to have to see what happens with the GDPR and the extent to which it addresses people's concerns and supports ongoing innovation.

It is very interesting that the previous data protection directive was quite enduring and lasted for 20 years. I am not as confident that the GDPR will be as long lasting, given that it is more prescriptive at a time when the world is changing more quickly. It will absolutely be a central focus for politicians and policymakers, because it is such a fundamental issue for our society.

Dom Hallas: I do not have much to add to that.

Q46 **Lord Gordon of Strathblane:** You made the point that something has endured for 20 years, but the pace of change, as you pointed out, has grown exponentially since then, and the problems/opportunities have increased. Can we still get by with the Safe Harbour idea that online platforms have no responsibility for what goes out online? Or do they have some responsibility, and, if so, is it a self-defining obligation, or are there external criteria that we can use to determine where in the spectrum they lie?

Antony Walker: The e-commerce directive was one of these fundamental pieces of enabling regulation that tried to strike a balance between appropriate safeguards and providing a legal framework by which companies and individuals could transact safely across in an online world. It has been pretty enduring. It was quite an enabling piece of legislation. It was not too prescriptive.

Having said that, there is a misunderstanding that there are blanket exemptions from liability in the e-commerce directive, which is not the case. The limitations are limited. They are also quite specific. There are specific instances where you have limitations of liability. If you move out of that, those limitations do not exist. Addressing this limitation of liability issue would be a panacea for a whole set of issues to do with rebalancing the role that some of the big digital platforms play.

We are less confident that that is the case, not least because it is an area where you make a change to address a particular problem in the digital world that you have identified, but you risk impacting everybody across the whole digital economy through to the online greeting card company. This is one where we feel that this is the wrong tool for the job. We are not saying that there is not an issue. We are saying that this feels like a sledgehammer to crack a nut.

Lord Gordon of Strathblane: The purpose of this inquiry is to try to find the right tools for the job. Can you help us? What should be done?

Antony Walker: Something that slightly concerns me about the current debate—and, if I may say so, the title of your inquiry—is that when we talk about the internet and harms, we are increasingly conflating many, many different issues. Concerns about bullying and terrorist content are confused with issues of competition law and monopoly. There are implications of AI.

A challenge that we have at the moment is that all these issues are becoming rather confused and rather conflated. Where your work could be incredibly helpful would be to try to segment that down to, "Here are a very specific set of issues that we are concerned about and about which we think there's a legitimate public concern" and we can look at finding the right solutions to those issues. That would be very helpful.

At the moment, there is something of a gap between the political rhetoric and the way in which some of these issues and concerns are discussed at a political level and in the media, and the policy reality, which is unhelpful for everybody.

Lord Gordon of Strathblane: When you referred to the political rhetoric, did you have in mind the Secretary of State's comments at the weekend?

Antony Walker: We have said publicly that we do not recognise this characterisation of the online world being the wild west. As I said, we have 20 years plus of specific legislation that applies to the digital world. What is illegal offline is also illegal online. We do not challenge that as a concept in any way. That is where the disconnect is. We would like to get much more into the detail, but at the moment there is a gap.

Lord Gordon of Strathblane: Let me assure you that references to the wild west did not come from politicians originally. They came from witnesses to our last inquiry from the advertising world, who described digital advertising as the wild west and produced a fair degree of justification for it.

Antony Walker: That is where I think we should get specific about the very problem that we are trying to address and not talk about the internet.

Lord Gordon of Strathblane: It covers a multitude of sins or virtues.

Antony Walker: Many virtues.

Dom Hallas: On that point about the e-commerce directive, I share Antony's perspective. Fundamentally, there has been extraordinary growth and development in technology businesses and internet businesses more broadly in the past 20 years. The e-commerce directive has been a fantastic legal basis for that conversation. It is important to realise that the directive does not draw a distinction between media businesses or tech businesses. If you have a newspaper, the online comments on your website are also covered by the same limitations of liability that a social media platform might be.

Equally, with Matt Hancock's app, for example, when he puts his own content on the application, it is not covered by the liability, but the users' comments are. It is important to get into the conversation about the exact specifics of the e-commerce directive. This is an interesting forum in which do so, because you have the ability to consider these things in further detail and the value that it adds to the internet economy.

The Chairman: Does it act as a disincentive on companies to take action?

Dom Hallas: To take action on content?

The Chairman: Yes.

Dom Hallas: I would flip it round. One of my big concerns about the e-commerce directive and the conversation about limitations of liability and the potential removal of them is that in many ways it would not address the challenge that people think it would. There is a lot of conversation from politicians about tackling tech giants through the removal of limitations of liability. In many cases, these companies are best placed to deal with the removal of those limitations precisely because they have the largest amount of resources and armies of lawyers.

Lord Gordon of Strathblane: Yet things happen that clearly should not happen.

Dom Hallas: Indeed.

Lord Gordon of Strathblane: Is that a failure of self-regulation?

Dom Hallas: It is partially a conversation about how best to regulate. One piece of legislation is not necessarily the conversation about the whole ecosystem, which is exactly Antony's point. There is a breadth of regulation on these issues, and it is about understanding which buttons to push as opposed to pointing one out and saying that it is a concern.

Baroness Kidron: Mr Walker, I feel a bit split in that you are saying on the one hand that everything is all right but be specific. As soon as you are specific, that is better dealt with by them because they will see it all right. It is a little confusing. On this particular issue about Safe Harbour, there is a "do not look, do not see" problem, is there not? Platforms take down content if it has been pointed out. They do not have to go and find it. It requires a member of the public or some other person to point it out. Is that suitable?

Antony Walker: We have moved on from that. We are already seeing the largest platforms using AI technology to identify material that is either illegal or very clearly harmful. As that new technology is being developed and implemented, we are seeing a significant increase in the amount of material that has been taken down before anybody has viewed that.

We have to be clear that where things are illegal, the context is clear and it is very easy to identify them—that applies in particular to child abuse content and quite a lot of terrorist propaganda content—it is very easy to be confident as a business about your decision to take that material down.

The public debate is not about that material; it is about things like hate speech and bullying, which takes you into material that is often language-based and highly contextual. How you read and make a determination about that is a much more nuanced issue that machines at the moment are frankly not good at doing. That is where you have to bring in the human decision-making.

Baroness Kidron: Could you not agree with me on this point? I completely agree with you. A nuanced way forward is what we all seek. Suddenly deciding that a big platform has responsibility for hate speech is not necessarily the answer. Have your members come to the table to engage with what a societal answer is?

Antony Walker: In the last year we have seen a significant stepping up of activity, such as: the Government's response in the Green Paper, which was published at the weekend, in which they recognise that the larger players are doing a lot more; the recent transparency reports that have been published; the kind of debate that we have with companies about those transparency reports where they are very clearly interested in taking views on what more could be done as they further iterate; and the very fact that companies are investing significantly in more resources and more teams.

Some of these companies were a bit slow. Many would recognise that. They are very quickly trying to change gear and address these issues. They are trying to be quite responsible in thinking about the broader implications of them moderating public debate online and talking to lots of NGOs and civil liberties organisations to try to gauge where they should be going to get the balance right. There is a lot of activity and behaviour that is very positive but is rarely portrayed in the broader debate. That is from my perspective. That is what I see.

Q47 **Lord Gordon of Strathblane:** I will follow up on the algorithm point now, because in many ways it might be the answer to the human element that you view as being required. Last week we had the Internet Watch Foundation, which made the point that it should have a human being adopting every algorithm that is used and monitoring whether it is doing its job properly. Would that be a start of an answer?

Dom Hallas: Broadly, the points that Antony made about the role of AI are correct. It does a very effective job at addressing things like child abuse images, where oftentimes these are images that are recirculated among the same networks; they are old images that you can re-analyse.

AI has more of a challenge precisely with the human element. One of my big worries, which cuts back to the competition conversation, is that if the answer is to encourage Facebook to hire 20,000 moderators, that is certainly not the answer for the rest of the digital economy. That would be my one big plea. The role that AI can play as it gradually develops in doing more of that work is very important.

Antony Walker: We are still in the early stages of the development and application of AI for these kinds of solutions. It works well when we are talking about images and video. At the moment, it is much less effective when we are talking about issues with language. Therefore, it seems highly likely that you will continue to need human moderation alongside the AI. The recent transparency reports show that the trusted flaggers approach works quite well. That is an example of where some of these large companies have been working with communities and engaging quite widely about how they build their solutions.

The technology will improve. The big question is about the smaller emerging platforms that do not have the kinds of resources that the very largest players have. There is some quite good dialogue and engagement between the big players about how they can share some of their technology. The Home Office and the Government have been working with third parties to see whether they can develop AI solutions that could be used by smaller players. I am quite optimistic about the role of AI, but we have to be very cognisant and aware of where we draw the line when it comes to the decisions that AI or these companies should be taking about the material that should or should not be online.

Lord Gordon of Strathblane: Are you content with a situation where in a way you are guilty until proved innocent, because the algorithm finds you guilty and a human individual might decide it was reasonable after all?

Antony Walker: The recent example in Germany is significant. Facebook took down some content in accordance with the new German law on hate speech and was told by a court that it had acted improperly. This is the sort of jeopardy that businesses are very concerned about and do not want to be caught in. They are conscious of the real significance of some of these discussions. Frankly, this is where policymakers need to be engaged, particularly in helping to define some of the issues about what is and what is not harmful content. This is where companies need help. It is not their job to make those sorts of determinations. There needs to be a public debate to help.

Lord Gordon of Strathblane: For clarification, if it is clear that something is harmful, it is their responsibility to stop putting it on their platforms.

Antony Walker: I am talking about instances where it is debatable whether something is harmful. Companies need the help of government and policymakers to help make determinations in understanding that line. If they are clear and confident about the decisions that they are taking, that enables them to react much more quickly.

Lord Gordon of Strathblane: The word for that is regulation, is it not? That is the help they receive.

Antony Walker: There are many ways in which you can do it.

Baroness McIntosh of Hudnall: You are on to something central to the discussion that we are having. For example, last week we were told that it was much easier to police and to have systems in place that could deal with child abuse images, because it was clear that the harm was defined. I am listening to what you are saying and asking myself whether what you want is not necessarily more regulation but more legislation. Is that what you are saying? Are you saying that it should be the business of policymakers and legislators to start trying to define what they mean by harm more rigorously than is currently the case? That appears to be what you are leading towards. That is a very big thing.

Antony Walker: Helping to provide clarity regarding how we determine these issues of harm absolutely will be helpful for businesses, which then have the responsibility to act. The Internet Watch Foundation is an interesting model that I would encourage you to look at and to think about why it has been so successful, because it absolutely has been. It is internationally leading in the way in which charitable organisations, industry and government have come together and worked effectively to collaborate to put a strong system in place for identification, takedown and subsequent prosecution in relation to child abuse.

Baroness McIntosh of Hudnall: We would entirely accept that. The point is that they work from an established body of law. You appear to be saying to us that there is a deficiency in the quantum of law that exists that would allow people in your sector to be more precise about where the boundaries are. Is that what you think?

Antony Walker: It is the case. The law may also struggle with some of these issues.

Baroness McIntosh of Hudnall: We cannot say it is too difficult.

Antony Walker: I am absolutely not saying that it is too difficult. I am saying that businesses need the help of government and legislators to think about how we can define that.

The Chairman: What we are stretching for is to define the device by which this certainty is created. We have talked about regulation, law and co-regulation, but the actual device by which the platforms and other companies have clarity about what it is society has decided is not acceptable.

Antony Walker: We are open to different approaches. There will be some areas where we can potentially provide a lot of clarity. There will be other areas where the challenge will be that we are working in legally very grey areas. The question is how you provide a bit more certainty that can provide better guidance. The law itself may struggle in some areas, but that should not stop us from trying to do a better job of defining norms in relation to harmful content and issues of harm.

Baroness McIntosh of Hudnall: Who do you mean by "us"? If it is not the Government through legislation, you would be pointing to—

Antony Walker: I do not think it has to be through legislation. It can be through codes. There are many ways in which we can do it. In some areas, legislation may be the better approach. We have not come that far in our thinking. I absolutely agree that we should be focusing collectively on government working together with industry.

The Chairman: You are posing a question and we are putting it back to you for an answer, to be fair.

Q48 **Lord Allen of Kensington:** You asked for specifics, so I would like to focus on the concern about the patents of algorithms and their use. In what ways would online platforms be more transparent about the impact of algorithms, how they are used and the impact on their users?

Dom Hallas: When we talk about algorithms, it is a question of what we mean by harm. When we dive down into the research and the polling about what people are concerned about, they are worried that algorithms and their data are being misused.

Lord Allen of Kensington: They are probably right to be worried from evidence we have taken and seen over the last number of months and years. Would you agree?

Dom Hallas: It depends on the specifics, but it is understandable if you have seen the debate in public over the last three months.

Lord Allen of Kensington: I will come back to the question of public trust, because another issue is what you will do about it. Mr Walker talked about the actions that you can take, but building trust is a significant issue, and I would like both your views on that.

Dom Hallas: On the point about algorithms, it is important to be clear that clarity about how data is used and clarity about what algorithms are being used for are not necessarily the same as pure transparency. My concern about what the Government published this Sunday in the *Internet Safety Strategy* is that the code of conduct is encouraging and suggesting that regulation might follow if platforms do not comply: a model where commercial platforms, including start-ups, are having to open up an awful lot of the kimono of their business to the public more broadly in a way that for a lot of UK-based start-ups that are growing platforms is genuinely very commercially risky when you have giant technology players that are buying up a lot of businesses. The internal workings of these companies are very commercially sensitive. We understand there are broader societal questions we have to address.

Lord Allen of Kensington: We are not talking about detailed programming. It is the purpose. What will this algorithm do? What is the impact on me, and how will it influence my behaviour or impact on me personally? We are not asking for the coding. That is the same point.

Dom Hallas: That is exactly what I mean. That is the distinction between giving clarity and giving what is often called transparency. Those two things are slightly separate.

Lord Allen of Kensington: In your evidence, Mr Walker, you talked about mechanisms. You did not favour legislation or regulation. Can you give us specifics on what sorts of mechanisms could be used to address this specific issue?

Antony Walker: The issue of algorithmic transparency is an incredibly live issue and debate across the tech community internationally, particularly as we look forward to the wider application of AI in society. There are clearly lots of situations where algorithms are taking sensitive decisions that impact people's lives where it seems entirely reasonable that it should be possible to explain why the algorithm made the decision it did. In fact, that is already written into GDPR in the right to explanation. Within GDPR it is unclear what that right of explanation means and the degree and extent of transparency that is required. It could require simply a top-level explanation—"It broadly said it took the decision for these reasons"—or it could require laying open the algorithm for full interrogation.

When you look to the wider application of AI and think of more autonomous machines operating where potentially something happens that should not have happened, being able to interrogate that algorithm to find out and understand why the outcome that happened did so will clearly be important in a society where we are so dependent on AI because it is embedded all around us.

The question is what that means in practice and how you resolve that issue. There is a misconception that all AIs are black box and you put data in and an outcome comes out and you cannot find out what is going on. That is not the case with most machine learning. It should be possible to be reasonably transparent to understand what happened with most machine-learning algorithms.

It is different for deep neural networks, where achieving full transparency may be more difficult. The research community is very focused on these issues and is looking at ways in which that kind of transparency, accountability and explainability can be achieved. In the world of computer science, this is an absolutely live issue. There are researchers around the world focused on these issues. As we enter into this next phase of living and working alongside smart autonomous machines, it is essential that we know why they are making the decisions that they make. It will be a big focus, particularly because we can see what is coming, not because of the examples that we see today.

Lord Allen of Kensington: If you come to the point that I made earlier about public trust, what specific actions should be taken to ensure that public trust?

Antony Walker: This is an issue that we have been—about around Ts and Cs being in language that the public can understand. The worry would be that you can explain it but that 90% of the population, including myself, do not understand.

Antony Walker: Cookies are a good example of a well-intended solution that fails to deliver the outcome that everybody wanted to achieve. How many times have we all clicked away the cookie reminder? Clearly, it was ineffective. Ts and Cs are clearly the wrong tool for the job. Ts and Cs are not a good way to explain to the user how a service operates. They are a legal requirement. They are there for a legal purpose. They are complicated precisely because of the legal requirements. Many companies have invested in thinking about how to make the relevant information available to the user at the point at which they need to know.

We did some work with the Competition and Markets Authority a couple of years ago. We took it through the process by which a number of our members have sought to take what is in their Ts and Cs and turn it into meaningful, timely information that is there at the right moment. I found what they have done quite impressive. Ts and Cs are clearly the wrong tool for the job when we are trying to think about how to make the way this service works understandable for people. There will be companies out there that want to hide behind their Ts and Cs, but good and reputable companies will want to make sure their users understand how the service works.

This brings me back to the question of ethics. We were a strong proponent of what has become the Centre for Data Ethics and Innovation. We are actively supporting the establishment of the Ada Lovelace Institute. We hosted a big digital ethics summit last year precisely because we think there is a whole new set of issues that is coming along whose ethics and norms we need to think through.

Once we have the ethics and norms right, we can focus in on, "What's the right tool for the job? How do we reach this specific issue there?" or, "We need a broad concept or framework that people can innovate under". There is a spectrum of activity from the very precise and targeted to the broad and general. We need to find the right mix of tools for that.

Q49 **The Lord Bishop of Chelmsford:** You helpfully reminded us that it is dangerous to conflate too many things together under this topic. Here is a specific question. In their written evidence to our recent inquiry on advertising, the News Media Association noted that Google and Facebook have bought companies whose applications might have challenged their market dominance. In your opinion, is the current competition law effective in regulating the activities of platforms in this regard?

Dom Hallas: At the moment, in the conversation on competition we are seeing perhaps understandable frustration at the pace at which the competition process works. When I think back to the way in which the European competition regulators have consistently addressed technology issues of the time, there has been an impact and they have made the effort to do so, but oftentimes, by the nature of the process being evidence-based, it has taken longer than ideally would have been the case, given public discourse and the pace of change.

I am by no means a competition law expert, I should add, but there is no doubt that it is an extremely complex conversation. At the moment, quite often the people who are having the discussion are not necessarily the best placed to do so. I make that broad point and bow out safely as a non-competition-based guy. Perhaps it would be worth consulting the new chair of the Competition and Markets Authority, who I understand will be joining you in the House of Lords.

The Lord Bishop of Chelmsford: So I understand, was that a yes or, "I don't know"? Is competition law effective?

Dom Hallas: Broadly it is effective, but it is perhaps slower than might be ideal.

The Lord Bishop of Chelmsford: So it is a yes.

Dom Hallas: Yes.

Antony Walker: Competition law gives us the best set of tools to address the way in which markets operate overall. There are two questions about competition law in relation to the digital economy. The first question is whether it can keep pace and keep up. Competition law is necessarily quite slow, but innovation and companies scale incredibly quickly. We have seen that over the last few years, and the question is whether it can keep pace.

The second question is whether it can cope with the economics of platform businesses. Platform businesses are not entirely new, but they have emerged as a fundamental shift in business models over the last few years.

When the CMA, under Alex Chisholm, looked at this issue in quite a lot of detail a couple of years ago when the European Commission was asking these questions about competition law, the CMA’s view was that it had all the tools in the toolbox. The fundamental doctrine of competition law was not the problem. The problem was more about the application and the need for competition authorities to make sure that they have a good and deep understanding of what is happening in digital markets, where maybe they have been a bit slow to understand that the economics of highly scalable platform businesses were different from the economics of other businesses.

Competition authorities can be quicker in sending signals to the market about what may be a desirable outcome. In a number of instances, the CMA has been quite good at signalling where it has a concern about something happening in a market. In itself, that leads to a correction before it has to intervene deeply in that market. Sometimes competition authorities could use those tools of signalling and say, “We are starting to see too much concentration here”, or, “We’re seeking outcomes here that we think are anti-competitive”.

The Lord Bishop of Chelmsford: That sounds like a no, or at least it is a “No, but they could be implementing it better”. Do you want to add anything about post Brexit in this regard, as a lot of the regulation currently comes to us through the European Union?

Antony Walker: Brexit is definitely a complicating factor. Ideally, we would want to see UK competition approaches continuing along the same path as European competition policy. Philosophically and with regard to the underlying doctrine, they are the same. I do not see why they should diverge, but there is always a risk. It is definitely a complicating factor. There are some who worry that the European Union could use competition policy in more of a defensive way; I do not particularly share that concern. The European Union has a very strong track record in tackling issues of market dominance and will continue to do so.

The Chairman: Do you agree, Mr Hallas?

Dom Hallas: Yes. It is one of the many areas where we all acknowledge the benefits of acting at scale. It is important that the UK competition authority continues to nod to Brussels as it continues to work.

Q50 **Baroness McIntosh of Hudnall:** This next question connects directly to what you have been talking about. It is about network effects, which appears to me, as somebody with no expertise in this area at all, to be directly related to the question of scale and new entrants into the market, how quickly they can scale up and whether further interventions are needed to make it easier for new entrants and smaller entrants to compete with the big guys who have the benefit of networking effects. I do not think that we need necessarily to spend a lot of time on this, given what you have said, but do you want to add anything on that issue?

Dom Hallas: This cuts to the much broader conversation that we have been having. Antony mentioned a little earlier the risk of regulation as a moat for the big businesses. I made a point about liability. One of the big challenges is in lifting liability, which might seem at first to address some of the challenges that might be presented by the big platforms. However, in many cases you would entrench their dominance precisely because their ability to control their network would be easier under heavier regulation.

The broader point to be made about the ecosystem is that we need to continue to have a sensible approach that will allow platforms and other networks to continue to liaise with each other. We see that technology businesses grow where there are other technology businesses. We always talk about the PayPal mafia in the technology industry, which is that the company PayPal had many of its children form other very successful companies. It is important to sustain that as well.

Baroness McIntosh of Hudnall: The ecosystem as you describe it has a lot of small players in it, but you also described—I cannot remember which one of you it was—a slightly predatory approach on the part of the large companies towards smaller companies. Somebody talked about them being hoovered up, as it were, by the big companies.

It has also been put to us that for many smaller companies—platform-based or not, but particularly platform-based—it is their aspiration to be hoovered up by the larger companies. How does the ecosystem allow companies to operate independently but also leave them in a place from which they can take advantage?

Antony Walker: This is a phenomenon that the competition authorities need to understand well.

The Chairman: Do they understand it?

Antony Walker: I am not convinced that they have been as attentive as they could have been to whether companies' ability to buy out their competition will cause problems further down the line. As you say, for many founders and many businesses it is absolutely an aspiration to be bought, and there is nothing wrong with that.

For companies that do not want to be bought out and that want to scale and grow, you want to support that as much as you can. Where you are intervening to distort the market in some way, you have to draw the line to clear the path for them. That is problematic. There is a real risk of creating a regulatory dependency for that company at a later stage, which often causes bad feedback problems.

Government can play a role in making sure that it is open to procuring from small companies and that it does not have a bias towards buying only from the large suppliers. You are not messing with the market in that way; you are simply being open to what small companies can offer.

Dom Hallas: When I made that point I was trying to say that it is important that the Government, in trying to intervene in one area, do not accidentally open smaller companies up to additional transparency that would encourage potential purchases and give larger companies much more information than they otherwise might have. If a company wants to be bought, that would be their right, and I believe there are many founders who would be very interested in doing that.

It is important to create an ecosystem where we can both encourage UK start-ups and scale-ups to become the next $10 billion company, but if someone else wants to sell for $1 billion, there is no problem with that. We would celebrate that as well and that is absolutely fine.

The Chairman: We have one further question. I will ask Baroness Quin to put the question on the record and ask our witnesses to reply to Baroness Quin and other members of the Committee in writing.

Q51 **Baroness Quin:** It is a wider question on Brexit in terms of what you both feel will effectively be UK's departure from the EU on this area. For example, Kodak expressed concern about continued access to the European Investment Fund. There were concerns raised with us about somehow being outside the EU's data protection framework and not part of that shared system. A more general but concerning question about the loss of influence by not having a seat at the table and, therefore, neither the UK Government nor British industry being in the negotiations at a crucial phase and losing out as a result. Those are the kinds of issues that I wanted to flag up.

The Chairman: The clerk will write to you and reinforce those questions, so you do not need to make a comprehensive note of them. I ask you if you would be so kind to reply to the Committee in writing. Can I thank our witnesses for shedding a lot of light on a number of issues for us around design and ethics, as well as competition law, which are at the heart of our inquiry? You are all working sensibly in this area. If you have further evidence that you believe would be of value to the Committee as your work proceeds, we would very much like to receive it and add it to our reading list. Thank you to both of our witnesses again for giving evidence today.

Jennifer Cobbe[650] and Professor John Naughton[651], Trustworthy Technologies Strategic Research Initiative, University of Cambridge – written evidence (IRN0031)

1. We believe that the Committee would benefit from information on the business model of many leading internet companies, known as 'surveillance capitalism' (a term coined by Prof Shoshanna Zuboff in 2015[652]). As such, this submission will describe surveillance capitalism, primarily focusing on Facebook as a typical example with reference to other companies where necessary. While the focus here is on Facebook, it should at all points be remembered that this business model is employed by Google, Amazon, LinkedIn, and many other online services that provide free services in return for the right to track users' online activities and monetise that data by enabling advertisers to target commercial messages at users whose compiled profiles suggests that they might be receptive to them[653].

1. The Origins of Surveillance Capitalism

2. Surveillance capitalism was invented by Google. Google's engineers realised that phrases entered by a user into their search box could be used (i) to predict what that user wanted (or was interested in) and then (ii) to sell to other companies the opportunity to target those users with advertising based on this prediction. This approach – which initiated in Google's core business of search – was later extended to other services offered by the company, notably Gmail and YouTube, which Google acquired in 2006.

3. Google has derived vast revenues and profits through surveillance, first by using it to sell targeted advertising in search and, later, by surveilling user activities elsewhere so as to predict behaviour more generally and maximise opportunities for profit in many other contexts. This is how the company went from being an unprofitable internet search engine in the 1990s to being a vastly profitable advertising company in the 2000s and one of the most valuable companies in the world in the 2010s.[654] In doing

[650] Department of Computer Science and Technology, University of Cambridge.

[651] Centre for Research in the Arts, Social Sciences and Humanities (CRASSH), University of Cambridge.

[652] Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization", *Journal of Information Technology*, 30, 2015 pp.75–89 [https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754]; Shoshana Zuboff, "The Secrets of Surveillance Capitalism", *Frankfurter Allgemeine Zeitung*, 5 March, 2016. [http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html]

[653] See Jennifer Cobbe, "Reigning in Big Data's Robber Barons", *The New York Review of Books NYR Daily*, 12 April, 2018 [http://www.nybooks.com/daily/2018/04/12/reining-in-big-datas-robber-barons].

[654] John Battelle, *The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture*. New York: Portfolio, 2005; Randall, Stross, *Planet Google: One Company's Audacious Plan to Organize Everything We Know*, Free Press, 2008.

so it invented the business model broadly followed by most of the companies which dominate the new digital world.

4. The origins of this – currently dominant – business model lie in the strength of network effects[655] in digital technology and the strategic imperative of online companies to get quickly to the point where they can exploit these effects. Because consumers are disposed to prefer 'free' services to ones for which they have to pay, the standard path to corporate growth was to offer free services – to make it easy for users to sign up by agreeing to permissive End User Licence Agreements (EULAs) which gave service-providers extensive freedoms to exploit users' data-trails and personal information. In this way we got to the situation where – as one prominent security researcher, Bruce Schneier, put it – surveillance became "the business model of the Internet".[656]

2. The Surveillance Business Model

2.1. Data Gathering

5. The first stage in the operation of surveillance capitalism is the collection and storage of large quantities of data about the everyday behaviours of hundreds of millions of people. The key here is obtaining as much data as possible about as many people as possible from as many sources as possible. The databases which hold all this data are at the centre of an extensive surveillance apparatus, holding a wide range of personal and behavioural information gathered through the monitoring of the everyday activities of users. The increasingly online nature of private, social, and economic life plays directly into this.

6. Some of this data comes from the personal information which is consciously and voluntarily supplied by users (information on their age, gender, location, relationship status, sexual orientation, etc.). However, significant amounts of this is *behavioural data*. That is, data describing the behaviour of users obtained through pervasive and extensive surveillance of their online activities. This could be, for example, data on which Pages have been 'Liked' by a given user; on which posts have been viewed by a given user; on identifying other users with whom a given user has interacted (including how many times, when, and for how long); on which posts, images, or videos have been seen or watched by a given user (including how many times, when, and for how long); on which advertisers a given user has interacted with (including how many times, when, and for how long), and so on. Virtually everything that a Facebook user does while using the service is recorded by Facebook.

7. Surveillance corporations often obtain personal and behavioural data relating to users from data brokers such as Axciom (these brokers

[655] Investopedia, "Network Effect" [https://www.investopedia.com/terms/n/network-effect.asp].

[656] Fahmida Y. Rashid, "Surveillance is the Business Model of the Internet: Bruce Schneier", *Schneier on Security,* 9 April, 2014 [https://www.schneier.com/news/archives/2014/04/surveillance_is_the.html].

themselves obtain data from many sources). There is a thriving market in personal and behavioural data which forms part of the ecosystem of surveillance capitalism and, to at least some extent, underpins many of the practices described in this submission.[657] (In the wake of the Cambridge Analytica scandal, Facebook has recently announced that it will no longer obtain data from some of these data-brokers[658].) In this way, surveillance capitalists construct a profile of each user (sometimes called a 'data mosaic') which can be extremely detailed. It has been reported, for example, that Facebook gathers 98 data-points on every one of its users.[659]

8. Surveillance of users is not limited to their behaviour on Facebook. In fact, Facebook members (and non-members[660]) are tracked across the internet, meaning that their activity beyond Facebook's website or app can be tracked and recorded by Facebook for the purposes of compiling extensive profiles of user behaviour. This is achieved in various ways. The most well-known of these is through 'tracking cookies'[661], which store a small file on the user's computer which allows them to be identified and their web activity to be tracked. Tracking cookies are increasingly being superseded by web beacons[662], which are usually small, invisible images on websites which track user behaviour and do not require files to be stored on the user's computer[663]. Facebook's implementation of web beacons is the Facebook Pixel[664]. Some companies have also been known to use 'device fingerprinting'[665], by which the unique combination of characteristics of a user's device (such as screen size, versions of installed software, and even lists of installed fonts) are used to track their behaviour. Facebook also obtains behavioural data from its subsidiaries, including Instagram and WhatsApp[666].

[657] John Naughton, "What Facebook's terms and conditions really ought to say", *Observer*, 22 April, 2018. [https://www.theguardian.com/commentisfree/2018/apr/22/what-facebooks-terms-and-conditions-should-really-say].

[658] Drew Harwell, "Facebook, longtime friend of data brokers, becomes their stiffest competition", *The Washington Post*, 29 March, 2018 [https://www.washingtonpost.com/news/the-switch/wp/2018/03/29/facebook-longtime-friend-of-data-brokers-becomes-their-stiffest-competition].

[659] Caitlin Dewey, "98 personal data points that Facebook uses to target ads to you", *The Washington Post*, 19 August, 2016 [https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you].

[660] David Ingram, "Facebook fuels broad privacy debate by tracking non-users", *Reuters*, 15 April, 2018 [https://www.reuters.com/article/us-facebook-privacy-tracking/facebook-fuels-broad-privacy-debate-by-tracking-non-users-idUSKBN1HM0DR].

[661] Tom's Guide, "Tracking Cookies: What They Are, and How They Threaten Your Privacy", 16 September, 2013 [https://www.tomsguide.com/us/-tracking-cookie-definition,news-17506.html].

[662] IAPP, "Web Beacon" [https://iapp.org/resources/article/web-beacon].

[663] Although they may be stored temporarily in the web browser's cache.

[664] Facebook, "Facebook pixel: Measure, optimise and retarget with Facebook ads", [https://www.facebook.com/business/learn/facebook-ads-pixel].

[665] Jeremy Hsu, "Top Websites Secretly Track Your Device Fingerprint", *IEEE Spectrum*, 11 October 2013 [https://spectrum.ieee.org/tech-talk/telecom/internet/top-websites-secretly-track-your-browser-fingerprint].

[666] Although WhatsApp recently agreed to stop sharing data with Facebook until it can do so in a way that complies with GDPR (Samuel Gibbs, "WhatsApp sharing user data with Facebook would be illegal, rules ICO", *The Guardian*, 14 March, 2018

9. The Internet of Things[667] (IoT) – including smart cities and in-home smart devices such as Amazon Echo and Google Home – is in fact an internet of eyes, ears, and sensors in homes, offices, and public spaces which are watching, listening, and gathering data about the behaviours of millions of people and feeding this information back into corporate databases. The potential future expansion of the IoT promises to dramatically increase the personal and behavioural data that these corporations can gather on their users.

2.2. Predictive Analytics

1. The second stage of surveillance capitalism involves inputting the vast quantities of personal and behavioural data gathered through surveillance of user behaviour to machine learning[668] algorithms with the aim of inferring insights into users from which predictions about their future behaviour can be made. This process is commonly known as 'reality mining'[669].

2. This involves informating – that is, producing information which is new and otherwise unknowable to the entity who is doing it[670]. By combining and analysing the data of millions of users, patterns can be identified, inferences can be drawn, and information about individual users can be predicted. For example, Kosinski et al[671] showed what analysis of simply what users had 'Liked' on Facebook could provide remarkably accurate information about them without access to any other information about those users. They found that even with this limited impersonal data they could use machine learning techniques to accurately predict users' sexual orientation, their ethnicity, their religious and political views, their personality traits, their intelligence, their happiness, their age, their gender, their use of addictive substances, and whether their parents were separated.

3. These practices mean that users and their behaviours, interests, social relationships, consumption preferences, and so on are not just visible to

[https://www.theguardian.com/technology/2018/mar/14/whatsapp-sharing-user-data-facebook-illegal-ico-gdpr].

[667] Nicole Kobie, "What is the Internet of Things?", *The Guardian*, 6 May, 2015 [https://www.theguardian.com/technology/2015/may/06/what-is-the-internet-of-things-google].

[668] A process by which machines can be trained to spot patterns in large datasets so as to identify correlations and make predictions without having to be specifically programmed to do so.

[669] "The collection and analysis of machine-sensed environmental data pertaining to human social behavior, with the goal of identifying predictable patterns of behavior." [https://en.wikipedia.org/wiki/Reality_mining].

[670] According to Zuboff, the ability to informate is the key difference between the 'smart' machines of today and 'dumb' machines of the past, which could only automate human tasks (see Shoshana Zuboff, *In The Age Of The Smart Machine: The Future Of Work And Power*, 1988, New York, NY: Basic Books).

[671] Michal Kosinski, David Stillwell, and Thore Graepel, "Private traits and attributes are predictable from digital records of human behaviour", *PNAS*, 110(15), April 9 2013, pp.5802-5805 [http://www.pnas.org/content/110/15/5802].

Facebook, but become *hypervisible*. Making users hypervisibility through predictive analysis is the key aspect of this second stage of surveillance capitalism.

2.3. Targeted Advertising

4. Taking advantage of the insights into user behaviour obtained through predictive analytics, surveillance corporations use behavioural nudging in the form of targeted advertising with the intention of directing user behaviour in directions desired by advertisers. Facebook sells access to knowledge about users (derived through surveillance and predictive analytics) and their weaknesses and vulnerabilities (derived through experimentation), as well as access to the targeting tools themselves, to other companies, political parties and candidates, and anybody else who will pay.

5. Nudging in this form is prevalent both on the web and in the mobile apps produced by companies such as Google and Facebook. Links and associated information are often determined algorithmically in order to induce a desired behaviour in the user, seeking to take advantage of known shortcuts in human decision-making (known as 'heuristics'). The fact that these nudges are both highly personalised[672] and dynamic[673] – neither of which is true of real-world nudges – leads Prof Karen Yeung to call them 'hypernudges'[674]. As Yeung puts it, with the personalised, dynamic, and responsive nature of digital spaces, "these nudges channel user choices in directions preferred by the choice architect through processes that are subtle, unobtrusive, yet extraordinarily powerful"[675].

6. This process is refined through continual experimentation with nudges in order to determine which are most effective, both in terms of the form of adverts themselves and in terms of the contexts in which they are provided. This takes advantage of the ability to learn from failure (i.e. by learning which adverts work on any given user *and* which don't). For example, Google as of 2014 ran about 10,000 experiments a year in its search business, with around 1,000 running at any given time[676]. In 2008 these experiments resulted in 450-500 changes in the system, tweaking

[672] In that they can be targeted to users or small groups of users.

[673] In that they can be altered in real-time in response to user behaviour – they can continuously update suggestions on the fly to account for changes in behaviour or to offer new suggestions in repeated attempts to induce the desired behaviour should those previously proffered be ignored by the user. As a result, they can dynamically provide more relevant and, in theory, more effective nudges based on changing circumstances and tailored both to take into account changing trends in the behaviour and responses of users generally and to reflect the variable and unique behaviour of the targeted individual specifically (Karen Yeung, "'Hypernudge': Big Data as a mode of regulation by design", *Information, Communication & Society*, 20(1), 2017, pp.118-136 [https://www.tandfonline.com/doi/abs/10.1080/1369118X.2016.1186713]).

[674] Yeung, 2017.

[675] Yeung, 2017, p.119.

[676] Hal Varian, "Beyond Big Data", *Business Economics*, 49(1), 2014 [https://econpapers.repec.org/article/palbuseco/v_3a49_3ay_3a2014_3ai_3a1_3ap_3a27-31.htm].

everything from the background colour of ads and the spacing between ads and search results, to the underlying ranking algorithm. As a result, when any given individual is using the internet they are likely the unwitting subject of dozens of experiments which are seeking to figure out how to most effectively target them with advertising and direct their behaviour in the way desired by advertisers.

2.3.1 Custom Audiences

7. Facebook provides a set of tools, known as 'Custom Audiences'[677], which enable advertisers to deliver targeted advertising. Custom Audiences allows advertisers to submit lists of specific individuals who they wish to target to Facebook, which then matches the entries on those lists to the Facebook profiles of those individuals. Custom Audiences then allows users to be algorithmically filtered according to desired characteristics determined through their profiles and the surveillance of their online behaviour and facilitates the sending of tailored advertising directly to those specific individuals.

8. Facebook also provides a tool for identifying 'Lookalike Audiences'[678]. This allows advertisers to identify other users, who are not on their targeting list but share characteristics with those who are, to target with the same advertising, potentially dramatically expanding its reach. As well as this, there is a 'Website Custom Audiences' tool, which allows advertisers to implant the Facebook Pixel in order to keep track of which Facebook users visit that website. Advertisers can then filter them and target those individuals as well.

9. At all times, whether using Custom Audiences or Lookalike Audiences, user engagement can be monitored, tracked, and analysed through the 'Conversion Tracking'[679] tool so as to identify which ads are most effective with which demographic, allowing advertisers to more precisely hone their message through experimentation.

3. News Feed

10. Social-media companies like Twitter and Facebook enable their users to post content (tweets, status-updates, photographs, videos) to their accounts which will then be visible to their 'followers' (on Twitter) or 'friends' (on Facebook). In the beginning each user was then provided with a rolling list of these posts, generally in chronological order. But as the business model evolved the rolling lists were algorithmically

[677] Facebook, "About Custom Audiences from customer lists" [https://www.facebook.com/business/help/341425252616329].

[678] Facebook, "About Lookalike Audiences" [https://www.facebook.com/business/help/164749007013531].

[679] Facebook, "Measure Conversions" [https://developers.facebook.com/docs/facebook-pixel/pixel-with-ads/conversion-tracking].

'curated'[680] so that users eventually came only to see content that met three criteria: (i) posts by their friends that the machine-learning algorithm inferred might be of interest to them; (ii) posts which might increase 'user engagement' (which creates monetisable data-trails); and (iii) commercial messages that the algorithm judged would be of interest -- based on analyses of users' data-profiles. Curating the News Feed in this way is a key aspect of the monetisation of users' social interactions.

11. Much of the controversy that has arisen concerning the political implications of Facebook and Twitter stems from concerns about the way this 'curation' of news feeds operated[681]. In essence, Facebook constructed an impressive automated system for enabling advertisers to target commercial messages at consumers who might be receptive to them. It did not seem to occur to the company that this system would also work well for actors seeking to direct political or ideological messages at social-media users.

4. Moderation

12. As the political impact of the 'weaponisation' of Twitter and Facebook became obvious the companies faced demands from legislators and others to take responsibility for content what appeared on their platforms, and to implement procedures and processes for moderating content deemed to be politically manipulative or unacceptable in other ways. Initially, these platforms pushed back against such criticism initially arguing that the percentage of such content was negligible and that in any event they were exempted from editorial responsibility by Section 230 of the 1996 Communications Decency Act.[682] When these protestations were shown to be unconvincing, the companies fell back on arguments about the impossibility of the task of moderating content on their platforms because of the colossal scale of their operations. When these arguments proved unconvincing to legislators and other interested parties, the platform operators began to emphasise the sheer impossibility of effectively policing content posted on the scale of their operations. One source[683] estimates the scale of the activity on Facebook *every minute* as: 510,000 new comments, 293,000 status updates, and 136,000 new photos. Clearly the task of moderating content on this scale is impossible. Although Facebook now claims that it will soon be employing 20,000 human moderators, the company's CEO is putting most of his faith in

[680] Kelley Cotter, Janghee Cho, and Emilee Rader, "Explaining the News Feed Algorithm: An Analysis of the "News Feed FYI" Blog", *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, pp.1553-1560, ACM [https://doi.org/10.1145/3027063.3053114].

[681] See, for example, Zeynep Tufekci, "How Facebook's Algorithm Suppresses Content Diversity (Modestly) and How the Newsfeed Rules Your Clicks", *Medium*, 7 May, 2015 [https://medium.com/message/how-facebook-s-algorithm-suppresses-content-diversity-modestly-how-the-newsfeed-rules-the-clicks-b5f8a4bb7bab]

[682] See John Naughton, "How two congressmen created the internet's biggest names", Observer, 8 January, 2017 [https://www.theguardian.com/commentisfree/2017/jan/08/how-two-congressmen-created-the-internets-biggest-names].

[683] Zephoria, "The Top 20 Valuable Facebook Statistics – Updated April 2018" [https://zephoria.com/top-15-valuable-facebook-statistics].

> being able to deploy AI technology that will automate the task. AI will definitely help, but most experts are sceptical that the technology will be up to the task in the foreseeable future.[684]

11 May 2018

[684] Siva Vaidhyanathan, "Techno-fundamentalism can't save you, Mark Zuckerberg*", New Yorker*, 21 April, 2018 [https://www.newyorker.com/tech/elements/techno-fundamentalism-cant-save-you-mark-zuckerberg].

Julian Coles, Doteveryone and Internet Society – oral evidence (QQ 28-34)

Tuesday 8 May 2018

Watch the meeting

Members present: Lord Gilbert of Panteg (Chairman); Baroness Bertin; Baroness Benjamin; Baroness Bonham-Carter of Yarnbury; Lord Gordon of Strathblane; Baroness McIntosh of Hudnall; Baroness Quin.

Evidence Session No. 4 Heard in Public Questions 28 - 34

Examination of witnesses

Rachel Coldicutt, Chief Executive Officer, Doteveryone; Julian Coles, Independent Digital Media Policy Consultant; Dr Konstantinos Komaitis, Director of Policy Development, Internet Society.

Q28 **The Chairman:** May I welcome our witnesses to this evidence session of our inquiry into regulation of the internet? Thank you to our witnesses for joining us, agreeing to speak to the Committee and bringing your expertise to inform us.

The meeting is being broadcast online and a transcript will be taken. There is a possibility that our session will be disturbed by votes in the House of Lords Chamber. If that happens, we will adjourn for about 10 minutes and ask you to wait for us to come back.

May I ask our witnesses to briefly introduce themselves and tell us a little about their background? In so doing, so we know where each of you is coming from, could you tell us what your thoughts are on whether the internet needs further regulation? If it does, from your experience what type of regulation should it be: some form of self-regulation, co-regulation or a more directed form of regulation? When we have done that, members of the Committee will ask a series of further questions.

Rachel Coldicutt: I am the CEO of Doteveryone. We are a think tank that champions responsible technology for the good of everyone in society. We think of responsible technology as that which is good for everyone, that considers its impact, understands its consequences and seeks to mitigate those. The chair is Baroness Lane-Fox, who I am sure many of you know.

We spent two years looking at how technology is changing the world. We are pretty unambiguously in favour of regulation. We have backed it up by asking the British public their opinion and by trying to understand their attitude to technology and their understanding of it. There is a clear appetite among the public for additional regulation, too. From our perspective, it cannot be solved simply by self-regulation, and there is potentially an issue with the Government taking on the whole regulatory matter, not least because the Government's views of the internet probably also need to be subject to regulation.

We are in favour of an independent body that understands how technology works and is supported by public education. It needs to be a body that people can turn to, because we have heard that nobody knows who to ask on standards and safety tests.

I would add two things. The first is that there has been an enormous amount of conversation about social media, but ultimately it is the tip of the iceberg. There are an enormous number of other potential harms. Whether it is to combat addiction, bias, discrimination or democracy hacking, the internet has to be regulated. There are probably three areas to regulate—big tech, emerging tech and public sector tech—and they all need slightly different approaches.

Dr Konstantinos Komaitis: Hello, everyone, and thank you very much for inviting me here. I am the director of policy development for an organisation called the Internet Society, and I will say a few words about it.

We were established in 1992 by the very people who created the internet, Vint Cerf among them. At the time, the reason was to provide the organisational home to a community of engineers called the Internet Engineering Task Force, which was creating the internet and the standards that made the internet grow and evolve. Over the years, the Internet Society has grown to become an organisation that touches on three areas: policy, development and technology. We are a mission-based organisation. However, we have individual members, chapters in most countries around the world as well as organisational members. As an organisation, we work to ensure the internet stays open, interoperable, global and secure.

On the question of regulation, I would like to make two comments. First, there is a misconception that the internet is not regulated or has never been regulated. That is not quite the case. There has always been regulation of the internet, whether we are talking about copyright, intellectual property, data protection and so on. On top of the regulation that exists, people have always come together and collaborated in a form of self-regulation, or even hybrid forms of regulation and in the development of norms. Especially when it comes to the latter, we are seeing more and more communities coming together to produce those norms. A clear example is the Global Commission on the Stability of Cyberspace, which is a multi-stakeholder group consisting of Governments, businesses, civil society and the technical community. They came together to produce norms that hopefully will be adopted when it comes to the security of cyberspace. They have just released a norm calling for the protection of the public core of the internet.

The second issue is that when we use the phrase "internet regulation", it is a little wide and we need to be a little more specific. The infrastructure of the internet, which essentially is the backbone of the underlying communications that facilitates the sending and receiving of packets of data, needs to remain open and free. There is no reason to regulate that, because voluntary standards support this infrastructure. They are market-based, they come out of multi-stakeholder consultative processes and they ensure that the internet grows and the technology grows with it. Regulation at that layer of infrastructure is not optimal and is not advisable.

However, as we move through the layers, this is where we see the behaviour that has generated calls for regulation, especially lately. There the question becomes how we can regulate it in a way that will not prohibit innovation and creativity. We can discuss this later in more detail. The question is not whether we should regulate but where and at what layer. As I said, we see particular behaviours at the application layer, and the question is who or what should be doing that.

As a last point, I would like to say that the internet is a by-product of collaboration. When it emerged, a lot of people came together because they wanted to create something that would allow them to communicate: essentially, to send packets of data from point A to point B. That was all that it was meant to be. Of course, right now we are in a completely different era, but the technologists and engineers working on the internet still view it as this idea that we want to transfer packets from point A to point B.

Where feasible, regulation of the internet needs to be part of a collaborative and informative process. It is true that the internet is a complex ecosystem. The input of the different stakeholders, especially those who have the experience, is very significant, and I would like to congratulate you for opening up this consultation process and seeking those inputs. Thank you.

Julian Coles: Thank you, too, for the invitation to appear here. I am an independent digital media policy consultant. I am sorry for the mouthful there. I have worked as a consultant with DCMS, Ofcom and the European toy industry. I am a trustee of Childnet International and I am on the Ethics Committee of the Internet Watch Foundation. For about 15 years, until three years ago, I looked after the BBC's editorial policy for its online and interactive services.

This is a wonderful open question. If you will allow me to, I would like to jump backwards a little and come from the past to the present. There is a great spectrum between self-regulation, co-regulation and statutory regulation. If we go backwards to where we have come from, I would start the clock running at about 1996 when the Internet Watch Foundation was created. One might call that a broadly self-regulatory initiative and one that in its own terms has been extremely successful at driving down the number of child abuse images hosted on UK servers. That is just one example.

I remember that when the Home Office task force came into existence in 2001, it was a multi-stakeholder approach, sponsored by the Home Office, to look at harm and offence and other things online. We churned out good practice guides on instant messaging, chat and moderation. They were pretty good and well worth having. That turned into the UK Council for Child Internet Safety, and we did the same sort of thing.

The last piece of good practice guidance that I worked on was the social media guide in 2015-16. What struck me about it was that it was designed to help small companies—SMEs, start-ups—and the good practice examples were provided by the great big tech companies. That was a perfectly sensible idea, but after the document was published you could not help but notice that there was no sustained attempt to follow up to see who took it, who used it, what they did with it and, crucially, what happened: what the effect was on the performance of the companies that this was targeted at and to what extent it worked.

At that point, two-plus years ago, I thought our run of useful and valuable self-regulatory initiatives and good practice guidance had got something wrong and we were not doing enough. Particularly when you think if we're looking at harmful and offensive content, there is no independent regulator. For some areas, this is covered-the Information Commissioner's Office and so on. That's particularly true for that area.

Last autumn, along came the *Internet Safety Strategy* Green Paper. The Government had the idea of an annual transparency review. I thought, "This looks really interesting, because here's the missing bit. Here's the bit that says the big companies cannot go on marking their own homework; they must have an independent evaluation". That is when the penny dropped for me. It is only in certain areas. We are talking particularly about social media and child protection.

At about the same time, the idea of the internet commission was born. I think you have a submission from us, or at least an outline of what the proposal is, but very briefly the thought is to take on the annual transparency review and provide a single common reporting framework. Different companies would provide information into this common reporting framework, so that if you wanted you could benchmark performance one against the other.

The intention as far as possible is to run a comparative analysis. The process would be independent of government, because we think there are some really tricky issues here, such as freedom of expression, which go beyond the safety side, where, yes, government will be an important stakeholder but it will be at one remove from the process.

Secondly, the intention is that where the work happens it should be in a neutral private space, so everything that the companies provide is not automatically published to the world. That is a space for dialogue, disclosure and evaluation, and ultimately an independent assessment and a first report. That first report would say what is working well, what is working badly, and, crucially—coming back to the start of your question; I am sorry it has taken a couple of minutes—what area from our evidence base may need more regulation. That might be statutory legislation, or it might be something else, but at least that would be evidence-based. There would be many months of rigorous debate and discussion, undertaken broadly in private, and out of that would come evidence-based recommendations.

Vicky Nash talked about procedural accountability when she came last week, and that is what we are aiming for and what we are working on. Yes, you look at quantitative figures, process and policy, and you ask, "How inside your companies, particularly in relation to social media companies, are you doing this stuff, because we don't know because you are not telling us. You are not being transparent and it is a bit of a black box".

I will give a couple of examples. In practice, how does the company decide what to remove and what not to remove? It is a very easy question, but the answers are going to be quite complex and subtle. It is then how the company measures and monitors the performance of human moderators and AI inside the company. They have their own metrics and they do quite a lot of this work; we just do not know what it is. In a rather discursive way, that is my response and an introduction to the internet commission.

Q29 **Baroness Bertin:** Building on that a little, in terms of the industry trying to do more in its own interests to avoid heavy regulation, can I ask a little about design of products? Baroness Kidron, who is not at this session, put down an amendment that you will be aware of on age-appropriate design. Can we have your views on whether that could have quite a big impact if done properly?

Julian Coles: Design is really important, and Baroness Kidron's amendment for the ICO to start looking at age-appropriate design for children is a very interesting idea.

Baroness Bertin: It is clear that children are a huge constituency.

Julian Coles: Yes, absolutely. One-third of humanity is under 18, as John Carr always reminds us.

Baroness Bertin: And the most vulnerable.

Julian Coles: Exactly. The design is shaped substantially by an advertising-funded model, to grab attention, to serve advertising and to collect data, but the design needs to benefit users and be for users and not put users at risk. Working on safety, privacy, transparency, consent and a fair and equitable exchange of value is an interesting idea.

Baroness Bertin: In reality, we are talking about dividing up the profit-making arm and the ethics. Do you think the industry is very receptive to that, or is it going to have to be dragged there?

Julian Coles: Things may have changed a little in the last couple of months when it comes to transparency.

Baroness Bertin: I wonder why.

Julian Coles: Quite. The threat of legislation always concentrates minds, and that is a difficult game of bluff. If you are doing an independent evaluation in the way that we have illustrated, if you have a stronger evidence base you can develop key indicators, which we have not done yet—we are in the middle of wrestling with those issues. Out of that could come, through procedural accountability, a more substantial test of willingness—the willingness to adapt, to change, to be much more open about how they work—so that third parties can measure independently how they are doing, because we do not know.

The Chairman: Rachel Coldicutt, do you have any insight into public opinion and what the public think of these issues?

Rachel Coldicutt: Absolutely. When we were asking people about their confidence in using the internet, it was extraordinary; people were marking themselves anything up to nine out of 10, but when we started to ask them how it worked, they said, "I don't really know". A lot of that is because things are easy to use and hard to understand, and that becomes more and more the case as we are looking at AI and voice. It is certainly not a matter of thinking only about children and adults. It is thinking about the cognitive load of, say, asking a person to understand everything that has happened after they have made an Amazon order or everything that happens in instant messaging. It is too much.

It has also come out that people have a deep feeling of ambivalence. There is a feeling that technology is helping them as individuals and it is not helping society as a whole. The conflict is: "I'm connected but everybody is walking around looking at their phones", which again plays into the addiction.

On design, the question is how to create experience that is transparent but does not overload, and how people can understand what is happening without understanding everything that is happening, because it is enormous. It is a question of how design can be more responsible and focus on individuals' needs and society's needs as opposed to simply driving advertising. An element of regulation at the level of design could lead to better outcomes in good behaviour, too.

Dr Konstantinos Komaitis: I do not have a lot to add. Both my colleagues have used the word transparency, and we should not underestimate the power of transparency and how important it has become. Users, especially after recent events, want to learn more, and they want to engage more and to know exactly what is happening.

Currently, the question that everybody is asking is: would we have signed up to those services had we known exactly what and how our data was used? Initially, we all understood that advertising is part of the business model. Platforms are offering free services, but they are businesses and they need to make money. At the same time, we did not have a very clear understanding of the extent to which how our data was used—or abused, for that matter.

Rachel raised a very interesting point about how we can give information to users but make sure that we do not overwhelm them with that information. Where is the balance of information so that users can make informed choices about whether they want to sign up to those services? The design plays a critical role in the ability to have built-in tools that allow this information to be given to users but in a way that facilitates their interaction on the platform rather than trying to change the platform itself.

Baroness McIntosh of Hudnall: I am very interested in what you are saying, Rachel, about the extent to which people need to understand what they have in their hands when they use their smartphones or whatever. I was thinking about whether, when you say that, you mean that they need to understand the technology, but I rather think you do not mean that.

Rachel Coldicutt: No.

Q30 **Baroness McIntosh of Hudnall:** At the same time, you have all made the point in different ways that people do not understand how the technology works. They do not understand it enough to be able to judge what is going on when they interact with it.

I would take the example of a car. It is a very naive example, but I find it helpful. You may not. Most of us probably know how to drive a car, and we are tested and licensed on our capacity to do so safely, but if I were asked, "How does this car work?" I would not be able to say. Increasingly, as the cars have become more sophisticated, I would be less able than I would have been 30 years ago to say how it works.

I do not know whether that analogy works at all for you, but in trying to grasp how we regulate how people behave in relation to this technology, which we do when it comes to using sophisticated equipment of other kinds, where do you see our responsibilities as users, not just our rights?

Rachel Coldicutt: I disagree that most people have an interest in learning more. People have busy lives, things are hard and the ease of technology is one of its problems. The driving analogy is close to my heart, because I am currently learning to drive. It is quite interesting, because in doing that I have learned quite a lot about how an engine works. I suppose over the years it becomes sublimated, you do not think about it and it is there in the back of your head. It is not that people need to learn, it is no one's fault, but there is responsibility on companies that are making money out of people's data to be extremely clear about the consequences of providing the data they are asking people for.

Currently, it is very hard for people to say that they do not agree to the terms and conditions of Facebook, partly because they are hard to understand and they are long, and because their lives are wrapped up in it, and there is no choice. Understandability to us is more about mental models and about "more or less" understanding how something works.

There is a chart that shows how advertising tech works. I do not know if anybody here has seen it, but it is enormous and it has 300 squares on it and arrows pointing everywhere. It is not possible for anybody to understand that, but it is possible to understand that your data is being used and personalised and monetised. It is about the level of understanding, I think.

Baroness Quin: To follow on, this may seem like a silly example but it has been worrying me since it happened just a couple of days ago. This sounds rather sad to say, but I was playing a word game on my phone and at some point something like, "Are you happy to share your contact list?" came up. I pressed "yes" instead of "no", and then wondered what on earth the consequences of that were. I was not able to find out and I was not able to go back.

The Chairman: Were all of us on it?

Baroness Quin: I do not think you were. Do not worry. It was rather an old contact list, in fact. Sometimes when you do something like that it will say, "Are you sure?", or, "This is what this means", but it did not say that at all. Is it as basic in some ways as ensuring that people are given more checks so that they know exactly what they are letting themselves in for?

Rachel Coldicutt: Yes, indeed, I would agree.

The Chairman: If that is the solution to Baroness Quin's problem, how do you codify that? If you say that is a solution, how do you get that imposed or adopted?

Rachel Coldicutt: I would say there are probably three elements. There need to be standards. I do not know if anyone has spoken to the Committee about dark patterns. Dark patterns are exactly as you describe. They are design patterns that encourage you to do things that you would not ordinarily choose to do. It would be relatively easy to have best practice standards to mitigate against those. There is then auditing and refining.

Looking at the research, just over half of people admit to agreeing to terms and conditions without even bothering to look at them because they are overwhelming. I would advocate looking at a number of key journeys and mandating patterns for design.

Q31 **Baroness McIntosh of Hudnall:** This is moving on slightly and is about the vexed question of the content—sometimes worrying content—hosted by platforms. The question of their liability for the content they host is very important, but they are very highly protected by the laws that were set up at the time the internet began to take hold.

To what extent do you think platforms should be legally liable, given the extent of their reach now, for the content that they host? Secondly, do you think that we need to have a new way of defining them? The distinction between publisher and platform is very crude in the current era. Is there some in-between state that we can identify and nominate that will help us?

The Chairman: We will adjourn the meeting for 10 minutes.

The Committee suspended for a Division in the House.

The Chairman: Baroness McIntosh had asked the question about the liability of platforms and I think Mr Coles was about to start the answers.

Julian Coles: A couple of months ago, I attended a whole day conference at Cambridge on intermediary liability, with the best academics and lawyers. I did not come out with a clear picture of exactly how to take things further. There was some very intelligent discussion, but one of the puzzles is that under the e-commerce directive, for example, we are told that there is no general obligation for platforms to go looking for illegal content. That is explicit and very clear.

Last September, the Commission came out with a communication that said, "Wait a minute. We are now very keen that you should promptly and speedily do precisely that: you should go looking for illegal content on your platforms, you will not lose your immunity and, if you don't do it, we will legislate". I said, "Am I confused?" and they said, "Yes, you are, but you are right to be confused, because no one knows what this means".

You mentioned platforms and publishers, and I suppose people have already come to the conclusion that social media, for example, is a sort of hybrid. I have heard people talk about whether it would be possible to split the host or the intermediary definition into an active host and a passive host. The passive host would be something like a cyberlocker where nothing really happens. There is not the busyness and the moderation and the AI buzzing along that you might have on somewhere like Facebook. If one were to try that, one would have to be very careful that it worked for the giants and the SMEs and the start-ups.

How do you get people to become unicorns and beyond from very little? It should not penalise platforms that actively manage their content. That is a tricky one. You could perhaps reward those with some sort of diminution in liability when things go wrong. I do not know. You also have to make sure that you do not give perverse rewards for taking down content when the content should not have been taken down. The freedom of expression side of things—the false positives—has to be weighed in the balance as you try to come up with a cleverer, more sophisticated and more focused definition.

Dr Konstantinos Komaitis: I would like to go back to when these exemptions on liability were introduced and why. Back in the day, it was—and still is—very important to ensure that every business that enters the internet and connects itself to the network is offered the same opportunities. That was essentially what the exemptions on intermediary liability were meant to do. It was a pivotal rule for a long time, and even today it has ensured innovation and competition. Imagine an environment where any new entrant could be liable for everything they were hosting. They would not be able to make it into this very highly competitive environment. This is particularly so for small and medium-sized enterprises in that they need to be able to enter the market and to grow. Thus, to an extent, we can argue that intermediary liability provides a level playing field for all entrants.

Of course, once you enter a market and begin to grow, this is when the questions start to become more interesting. Your behaviour begins to change as you move from being a platform that hosts content to a platform that does so much more with content. We need to think about the threshold where suddenly you are no longer just a platform but you are becoming something completely different and bigger, and it is not just hosting content; it is curating content, publishing content or managing content in general.

I know that I am not answering your question categorically, but it would be very dangerous to create a blanket rule where intermediary liability was scrapped off for every company, or every platform was treated the same when it comes to liability issues, because we would see fewer and fewer businesses emerging, which would mean less and less innovation, and ultimately it could affect competition.

Rachel Coldicutt: I would add that content is a bit of a distraction. The content that is published online by people and shown on social media is a symptom of the original problem, which is the underlying business model, and how the services are designed to encourage people to behave. While there is the issue of coping with the fire hose of content that is created and shared every day, we should be looking at the business models underneath that are encouraging people to create content that is pernicious, bullying and those other things. If there is an issue of liability there, I would say that it is about changing the models and the ways in which people are encouraged to share content and return to it over time.

Q32 **Baroness Benjamin:** One of the Government's Digital Charter's key guiding principles is that people should understand the rules that apply to them when they are online. We know that young people, for instance, exchange material that is unsuitable and they do not quite understand that that is an offence. They are not quite conscious of their actions.

The charter commits the Government to protecting people from harmful content and behaviour and working with industry to encourage the development of technological solutions. What role should users play in establishing and maintaining online community standards for content and behaviour? What initiatives should be undertaken to ensure that all users are digitally literate and aware of their online rights and, more importantly, their responsibilities?

Dr Konstantinos Komaitis: In determining the role that users are playing in this ecosystem, we need first to make a distinction. It really depends on the type of platform. That is the starting point. There are some closed platforms where users are much more active and they are able to set those rules and self-regulate and, ultimately, to self-govern and create those best practices that can move on and evolve. Wikipedia is a very clear example. Users are self-governing and there are very specific rules about entries and mistaken entries and about when a Wikipedia participant gets excommunicated from the platform depending on how many times they have failed to adhere to the rules.

There are also more open communities such as Facebook where the user does not necessarily have the ability to self-govern. There we see the increased responsibility of platforms kicking in in making sure that users are engaged, bringing them in as much as possible and making them active participants. We saw this recently with the flagging of illegal content. We see users being more and more active in flagging up illegal content and asking for it to be removed and so on.

There needs to be greater effort to involve users, but before we do that there are a couple of things that need to be done. First, we need to re-instil trust. The idea of trust is more important when it comes to the internet. Recent events, even events before that, have made us question the trust that we place in the internet, in the platforms operating and in everybody involved. This comes back to transparency. We will come back to that word a lot, because it is so very important and it is becoming more and more important.

The second point is how you empower users so that they want to participate and be part of that. We need to look at accountability and how we can create accountable processes that will carry users with them, which at the same time users know will be at their disposal to be able to address those issues.

Baroness Benjamin: Where does WhatsApp sit in your thinking? The other platforms that you have mentioned are quite open, but WhatsApp seems to be a very closed area with content that is not really suitable for people to be creating.

Dr Konstantinos Komaitis: WhatsApp in particular is an instant messaging communication medium in which you are creating content that you are exchanging between a group or one on one. It is not similar to Facebook, for example, which is an open platform. I think you are referring to the secretive communication that is happening through WhatsApp, if I understand you correctly.

Baroness Benjamin: My feeling is that you are driving people away to another area that is almost underground. Should we be focusing on that? A lot of people use WhatsApp, and racism, sexism and all kinds of issues have been happening on that platform. Have you thought through how we can embrace platforms such as WhatsApp as we move forward?

Dr Konstantinos Komaitis: I am not sure I fully understand your question, because WhatsApp is an instant communications medium between people, and the conversations are secret because they are encrypted. That end-to-end encryption is important to safeguard a lot of people who want to communicate secretly—and, yes, you are absolutely right that, as on any other platform, both online and offline, not very nice things sometimes happen within those apps.

This goes to your second question about how we get to a place where users are digitally literate and can flag this up and address those concerns. The other panellists might be better able to answer that, but there needs to be a lot of education.

The Chairman: Rachel Coldicutt, could you look at this burden of additional responsibility from the point of view of the user?

Rachel Coldicutt: First, the problem in communities that moderate themselves is that privilege tends to be afforded to people who are already privileged—people who have apparent authority in their offline life. Wikipedia has a problem in that it is not very diverse. It does not represent a large number of women or people of colour.

When it comes to platforms such as WhatsApp, we have heard that people do not know who to turn to. At the moment, if something goes wrong in their online life, people do not know who to go to. Is it a police matter, do they go to the platform, or is it even a legal problem? There is an issue there about transparency of escalation and a duty of care to the people. Equally, though, there is the problem of people not wanting to admit that things have happened, so there is a vulnerability there, too.

On the question of research into people's appetite to learn more, we have found, as I said, that people are pretty overwhelmed and that there is certainly a case for public health, as we are terming it. Rather than thinking about digital literacy and turning over the responsibility to every individual to look after themselves, it is more about a level of social awareness of how technology works and how to behave.

Public Health England's mission is interesting. It says, "We exist to protect and improve the nation's health and well-being, and reduce health inequalities". A digital alternative to that, which looks after people's health and well-being and gives them a place to turn to, seems like an attractive model. It should not be all about putting the onus on every individual to understand everything and to be doing the job of the platforms; they should understand who to turn to.

Lastly, in the questions we asked the public about regulating the internet, there was a huge appetite for a consumer body. Over 60% of people thought that there ought to be one. There was a lot of faith in the idea of, say, Which? being a body they could turn to. The Government were felt to have a role but perhaps not the capability.

Baroness Benjamin: A couple of weeks ago, Jeremy Hunt came up with a question about organisations such as Facebook taking responsibility. Do you think the Government should be taking that up or that, really and truly, it should be the various platforms taking up that responsibility?

Rachel Coldicutt: I would say that the Government need to create a culture of responsibility. The change that would have to be made in each of the platforms to move to that is enormous, so there need to be big regulatory incentives.

Julian Coles: Clearly, when you are talking about users and how they can make a contribution and take some control, there are user reports, trusted flaggers and feedback through academic research. End users have a vital role when it comes to the transparency reporting process. You need to look not at what happened in the creation of the report but at the outcomes, and how that creates sensible discussion and debate about the lessons we learn from what we have discovered as part of that process.

In terms of digital literacy, if you are looking at children, there are some excellent programmes—the Childnet Digital Leaders Programme, Parent Zone, the NSPCC—about creativity and critical thinking. It is not just to do with online, with the internet or with social media; a young person growing up in this world has to be equipped with critical thinking. That is fundamental and it runs right the way across the piece.

That does not let industry off the hook and is a really important point. We come up with great media literacy programmes, and companies do their bit and they provide money, but the companies need to take on more responsibility than they do at the moment. Ofcom, in its latest media literacy report for adults, reports that something like 19% of adults in the UK believe that if there is a search return on Google, and it is produced and revealed and comes up on your browser, Google have, to some extent, checked the accuracy of that piece of content. Last year it was 21% so it has gone down a little, but that is a really worrying statistic when one is talking about news, current affairs, elections and all that stuff.

It would be very easy to make it possible for ordinary users to click and get a sense not of the algorithms or the black box but of the key principles of a search and how the ranking is created. It is exactly the same for Facebook and social media news feeds; more and more young people are getting their news from social media news feeds, and some simple explanation of the principles behind the working of the algorithm would be really useful. That is equipping people with some essential tools when weird things happen, conspiracy theories rise to the top on a search engine and so on. I think that might help.

Baroness Benjamin: Who should do that?

Julian Coles: The companies that are running these critical services that we all use every day without thinking too much about should be under an obligation to make it really easy for the ordinary users to find out with one click how these things work.

The Chairman: Is it a moral or statutory obligation?

Julian Coles: I would hesitate to say that it should be a statutory obligation. This is one of the many things you could feed into the transparency review. It is about transparency and about informing the public. They can then decide whether they want to take the risk and what the implications of that might be.

Rachel Coldicutt: The likelihood of anybody looking at that is incredibly low. It would be cosmetic and would cover the company, without giving any further information to anyone who needed it.

The Chairman: Because people just would not engage with it. It is back to the issue of engagement with these tools and opportunities when they are out there.

Rachel Coldicutt: Because everybody expects speed and ease.

The Chairman: At the moment, when you are using the internet or you are on a platform, you are just concentrating on using it and you are not thinking about these things. When you are not using it is when you engage with the wider issues.

Rachel Coldicutt: Yes.

The Chairman: Thank you.

Julian Coles: I would add one thought. A lot of people I talk to—looking at academics, who are really across this, and people doing PhDs on cyberbullying and so on—have not found it easy to access the information on the key principles of how the algorithms work. The majority of the population will not necessarily pick that up, but if you are not making it feasible for academics and policy experts to get their hands on this stuff and have a sensible debate about it, perhaps there is some way to go.

The Chairman: That is a very interesting issue that we have discussed here. We move on now to Baroness Quin.

Q33 **Baroness Quin:** I am not quite sure what level of regulation is best and whether it should be national, European or even some kind of international regulation, if such a thing were possible.

My question is specifically about the European Commission code of conduct on countering illegal hate speech online. What thoughts do you have about this? Is it fair, effective or transparent, or none of those?

Dr Konstantinos Komaitis: I did some research on that before coming here, because I wanted to get some numbers. My research at least shows that things are getting better, perhaps not as fast as many would like, but things are getting better by the year.

There have been three reviews: one in 2016, one in 2017 and one at the beginning of the year. The results of the third evaluation show important progress. Some 70% of notified illegal hate speech is removed by IT platforms compared with 59% in the second evaluation and with 28% only two years ago. The agreed timeframe for reviewing notifications—24 hours—is respected in the majority of cases. The research shows 81.7%, which is twice as much as in 2016 when it was down at 40%.

The other interesting thing that seems to be coming out is that reporting systems, transparency of reviewers, and co-operation with civil society organisations have been ameliorated. Concerning the transparency towards users, a positive trend has also been identified in respect of the fact that, in 68.9% of cases, feedback is given to the notifying users. I think we are getting there.

Co-operation and collaboration help. This is a very clear example of where you see collaboration between users and platforms. Also, you see the platforms coming back and addressing some of those challenges. There is always room for improvement, but I think we are getting to a stage where both users and platforms understand the critical issues and how critical it is to find solutions to them. However, it is certainly taking time.

Baroness Quin: Do Julian or Rachel want to add anything based on their awareness of this?

Rachel Coldicutt: I would only add to your point about regulation at different levels that there is an issue of different cultural expectations in Europe and the US. One of the defining differences is the approach to freedom of speech. That means that a common framework between here and the States is harder to achieve than one between here and Europe.

Baroness Quin: That is interesting. Do you have any thoughts, Julian?

Julian Coles: Just one aside, which is that I have heard Facebook say twice in the last few months that it is struggling with a definition of hate speech. It was asking other people, "Please come and help us. We don't think we have the right answer. It's a really difficult problem. We could do with a hand", which I thought was an interesting example.

Baroness Quin: Is that part of the issue I was also going to raise about trying to get the balance between safety on the one hand and protection of the rights of freedom of expression and freedom of information on the other?

Julian Coles: That is really important. We know there is great pressure on the platforms to remove more harmful and illegal content and remove it more quickly, but at the same time how are we going to check whether content should be removed or should have been removed? Is there the right to complain? Is there the right of appeal?

When you ask the final question, which is how you check the impact of AI on the removal of content, we know from YouTube and the recent transparency review, that last June 45%[685] of violent extremist content was spotted automatically by AI. AI was the spotter. In December, it was up to 98% spotted automatically by AI. This is YouTube's own figure.

That sounds very clever, but the essential question I would ask is whether a human being then checks that this is correct or not. When does a human being check and when do they not? That suggests to me that there could be real value in some kind of independent batch testing/observation. We do not want them to be policeman, judge and jury. Obviously, they are not going to get it 100% right, but we could match the risks and the difficulties with what we know about AI, which is imperfect and not as great at context as it might be. YouTube, very transparently, has just said, "With AI, we are going to move beyond violent extremism to start looking at child safety and other areas as well".

Our commission has started to look very hard at procedural accountability and to think about how we can dial into this, not in trying to force the companies to spew their secret algorithms to the world but in trying to find out, "How are you monitoring this stuff? Why should we trust you?"

The Chairman: Rachel Coldicutt, do you have any evidence? You talk to users about the balance of their fears between the harms and freedom of expression. Do users talk and worry about freedom of expression?

Rachel Coldicutt: Not really. People are more concerned about their level of connection to their friends and family. We have found that people feel very uncomfortable about bumping up against things and that there is a feeling of helplessness. You have a neighbour who you have known for 20 years and it is only when you are friends on Facebook that you are aware of their interests, which you perhaps are not all that interested in. People feel they cannot totally control the things that they see.

Slightly more concerning to me is algorithmic moderating, because an algorithm is only as good as the terms it is set. Enormous bias can be encoded within that. If Facebook or others are determining their own meanings for hate crime, the problem is that there is no transparency in the algorithm. Those are the kinds of things that ought to be taken out of the business and agreed separately.

Lord Gordon of Strathblane: I am sure the answer to that is a human court of appeal, as it were, which must act fairly immediately. The argument is whether you exclude on an algorithmic basis and attempt to

[685] The witness later wrote to the Committee: "I misquoted YouTube's figure for June 2017. It is 40% not 45%". See Google, 'YouTube Community Guidelines enforcement': https://transparencyreport.google.com/youtube-policy/overview [accessed 23 July 2018]

win on human appeal or whether you allow it through and use the human appeal to get it back.

Rachel Coldicutt: There is a school of thought that there ought to always be a human in the loop in algorithms and every algorithm ought to have a named individual who is ultimately responsible for the parameters.

The Chairman: That is interesting.

Baroness Bertin: Because of the volume of traffic going through, in reality the amount of resource that will be needed to be redirected to police this, for want of a better word, is pretty big. I would like to know your views on that.

Julian Coles: I have been wondering and worrying about this. The algorithm is a response to the scale and speed problem. Very rapid progress has been made over the last six months in this one area, from what YouTube has told us. People are starting to push the boundaries all across. We have to keep a very careful eye on it. That is why I thought something such as batch testing could be used. You cannot appeal every decision, but batch testing is done independently, so you get in there and you say, "Okay, we will look at a hundred decisions or a thousand decisions out of a million and unpack them". They may be doing this themselves. I do not know.

Baroness Bertin: I have one very quick point. I know that this is not where we are at yet, but do you think there could ever be a product where the algorithm stops the image going up in the first place?

Julian Coles: That is already happening with hash testing.

Baroness Bertin: Presumably not enough though.

Julian Coles: It is most used where there is a known child abuse image. It goes into the hash bank and there is a lot of collaboration across different companies to say, "Right, we have this bank, we are sharing the bank", and it does not go up a second or third time. In a way, that is easier than origination.

Baroness Bertin: Yes, of extremist views.

The Chairman: To go back to Rachel Coldicutt's suggestion, you were suggesting, I think, that there should not be constant human intervention in what an algorithm is doing but that every algorithm should have a master, a human person responsible for what it does and accountable for that individual piece of programing.

Rachel Coldicutt: Yes.

The Chairman: Thank you. That is an interesting suggestion.

Q34 **Baroness Bonham-Carter of Yarnbury:** Picking up on that, we keep being told that AI is going to mean there are no jobs for humans, so I think we have created one here. Being serious, you were talking about resources, but this may well be a solution that is a good balance.

I am going to ask about something slightly different, which goes back to Baroness Quin's point when I first walked in—and apologies for being late—about inadvertently sharing her contact list. What information should online platforms provide to users about the use of their personal data? To what degree does the GDPR provide sufficient protection for individuals?

I also have a slightly tangential question, which I have asked before but I would be very interested in what you three think, about the misuse of a person's reputation, which is slightly different, to falsely sell things online. There are a couple of different questions in there. I know, Rachel, that your organisation has shown that 83% of people surveyed are extraordinarily ignorant, if that is the right word, about how their information is collected and what is done with it.

Rachel Coldicutt: Yes. It is clear that over 90% of people say it is important to know their data is secure, but only 40% of people claim to understand how their data is used, so there is a huge act of faith there. People are interested in knowing, but more than half of them cannot find out how it is being used. Some 70% of the people understand that data about them and research is collected and they understand that the website they have looked at has collected it, so there is quite a high understanding of active use, but there is a really low understanding of passive data, such as location and other things they are asked about the interaction we have with others. There is a very low understanding of that and how to control it.

The potential problem with GDPR is that it is not very actionable to me as an individual. If terms and conditions are not written in an understandable way, the likelihood of reading them remains low, to be honest. If my data is available, how do they get it? Is it my data? Is it the data of others I have spoken to? How do I look after it? How do I share it? There are lots of practical problems that come out of it, and given that most of the people do not really understand data as a term—it tends to be thought of as the package on your phone as opposed to the information about you—the likelihood of people knowledgably and intentionally asking to have their data looked after securely and being able to fathom it is low.

Dr Konstantinos Komaitis: A main issue in the current state of affairs, especially when it comes to platforms, is its centralised nature, where the data from and about the user is literally transferred to the platform provider, which results in a loss of control by us. We do not know what is happening, and on top of that there is the sense that it is an all or nothing situation. If you want to be part of a service, you need to do certain things, and there is no room for negotiating or even making it bespoke to your own needs.

Users are starting to demand to understand where their data is going and how it is being used. I mentioned already that at the beginning of social networking we all gave our information and we knew to an extent that that was part of the bargain: it was going to be used by advertisers, but we were part of the pool. Recent events have demonstrated that there are so many dimensions to how our data is potentially being abused. It is crucial that information is presented in a simple and comprehensible manner, because currently that is not the case.

You have heard all of us saying that the terms of reference are these long lists of never-ending pages that you do not understand. I have a legal background and I have to admit that occasionally when I read them I have no idea what the hell they are talking about. I can imagine people who are not digitally literate or who do not have a law degree will be even more confused. That is the first point.

The other point is that the information needs to be accessible and easily obtainable. We saw, especially in the beginning—again, it is getting better—that information was not so readily available. We often found ourselves trying to navigate a very complex ecosystem to get to that information, and even if we found out where it was we were not getting it. I would be a little conservative in my attitude to GDPR. It is coming into force in the next couple of weeks, on 25 May. At a fundamental level, GDPR tries to give users back control.

The Chairman: We will adjourn the meeting and, sadly, that probably means that we will not have an opportunity to come back, because we have already well extended the time we promised to keep you. We have one further question and we ask the clerk to write to you and ask you to complete your answers on this question and respond to one further question. We will close the meeting with thanks to you for your evidence, which has been very useful.

Competition and Markets Authority – oral evidence (QQ 135-142)

Tuesday 9 October 2018

Watch the meeting

Members present: Lord Gilbert of Panteg (The Chairman); Baroness Benjamin; Baroness Bertin; Baroness Chisholm of Owlpen; Viscount Colville of Culross; Lord Goodlad; Baroness Kidron; Baroness McIntosh of Hudnall; Baroness Quin.

Evidence Session No. 16 Heard in Public Questions 135 - 142

Examination of witnesses

Dr Andrea Coscelli, Chief Executive Officer, Competition and Markets Authority; Simon Constantine, Director, Policy and International, Competition and Markets Authority.

Q135 **The Chairman:** Welcome to our second session this afternoon of the House of Lords Communications Committee inquiry into internet regulation. Our second set of witnesses is from the Competition and Markets Authority. Mr Constantine and Dr Coscelli, you are both very welcome. Thank you for giving up your time to be with us. Today's session will be recorded, and a transcript will be made available.

Could you briefly introduce yourselves and tell us a little about the role of the CMA, your respective roles within it, and the current role of the authority, particularly in relation to the online regulatory framework? Do you have the resources and powers that you need to fulfil that role? Perhaps you would address those points in your introductory remarks.

Dr Andrea Coscelli: I am the chief executive of the Competition and Markets Authority.

Simon Constantine: I am the director of policy and international at the CMA.

Dr Andrea Coscelli: The CMA is the competition authority for the general economy of the UK, so we are different from Ofcom or other regulators. We have a wide remit. We have four main clusters of activity, all of which are relevant to the discussion today. The first is merger control. Jointly with the European Commission, we review mergers and acquisitions that affect UK consumers. There is a division of labour. Some of the large global European transactions are currently reviewed by the European Commission and we tend to look at national transactions. That will change after Brexit, and on current assumptions all those cases will come to us.

The second cluster of activity is competition enforcement, which is essentially the prohibition in competition law from engaging in abusive behaviour or illegal agreements. Today, again, this is done jointly with the European Commission. For instance, the recent cases in Brussels involving Google Shopping and Google Android protect UK consumers in many ways. As you know, the UK digital market is very large in Europe, so quite a lot of the commerce affected by such cases is in the UK. Again, there is a division of labour. At present, we focus mainly on national cases and cases involving Google or Amazon are dealt with in Brussels. That is again likely to change post Brexit. It might change in the next few months or a bit later.

The third area is consumer enforcement, which is done more at national level, so it is an area that is less likely to change. It has been a fairly active area for us, in particular in digital markets. For instance, we have an ongoing investigation into a secondary ticketing website. We are currently in court with a company called viagogo to try to get it to comply with UK consumer protection legislation; we are active in online gambling, working with the Gambling Commission; we are doing some work on hotel booking sites; and a few months ago we concluded some work on online dating. So quite a lot of our work is in digital markets.

The final area is market work, which is essentially a cross-cutting market-wide initiative. This is a fairly flexible tool, because it allows us either to look at the way competition works in certain markets and issue recommendations to government to introduce legislation or regulation, or potentially to launch a second phase where we can try to impose change by our direct order-making powers. For instance, in the context of retail banking, some work that is now taking place on open banking, linked to some of the discussions about platforms, arose through our own direct order-making power. Those are the four key areas.

On the final part of your question about resources and powers, we are a well-funded agency. We had detailed discussions with the Treasury, and our sponsor department the Department for Business, Energy and Industrial Strategy in the context of Brexit. We have had a significant increase in our resources this year to prepare for Brexit, and there is certainly an indication that we will be properly funded going forward. Obviously, there will be a spending review next year, so we will have to see exactly where we land on that.

Like our colleagues at Ofcom, the main challenge is to try to translate funds into expertise and skills in the agency. We are doing quite well on some of our more traditional skills. On the legal and economic sides we are recruiting quite well. We are convincing a number of colleagues potentially to come to us from private practice and take a pay cut; we try to explain the benefits to them and the general public of spending some time in an agency.

Digital is a different level of challenge. We have recently recruited a head of data and digital. We have been very happy about that. We are now trying to support him in expanding that area. We are trying to be creative through secondments, apprenticeships and universities. We are trying to be pretty flexible in the way we do it, but we will have to see in the next year or so where we land.

The Chairman: Mr Constantine, do you wish to add anything?

Simon Constantine: Not to that point, no.

The Chairman: Let us stick with your remit and your relationship with other regulators.

Q136 **Baroness Quin:** This is a similar question to the one I asked Ofcom. It is about whether there are areas of remit overlap between yourselves and other agencies; whether you have identified gaps as regards the issues we are looking at; and in either case whether you see the need for some kind of overarching co-ordinating body.

Simon Constantine: As you say, some of it was covered by Ofcom, but there are probably three main strands. Within the CMA itself, as Andrea has already noted, we have a number of different powers. Certainly, in the digital space there is a lot of overlap between them. A company that is in breach of consumer protection requirements might equally be violating competition law. Similarly, with our markets powers we are able to look at both competition and consumer issues. Within the CMA, it is about working out what is the right tool for the job.

As I think your question was getting at more directly, we then have the relationship with others. Splitting that between competition and the consumer: on the competition side you heard from Ofcom about the concurrency system we have with the sector regulators, the discussion that goes on with them about how cases are allocated and the co-ordinating mechanisms, such as the UK Regulators Network and the UK Concurrency Network that the regulators and the CMA are involved in, to work better together not only on specific cases but on research projects and things such as that.

On the consumer side, the other main enforcement body, along with some of the sector regulators, is Trading Standards. Again, there is an attempt to co-ordinate that through what is known as the Consumer Protection Partnership at national level to ensure coverage of all the issues. The CMA's focus is on the market-wide systemic issues, particularly those that affect consumer choice; some of the more local issues are taken forward by Trading Standards.

Baroness Quin: Do you think the current system is working? In your contacts with government are you pressing for changes to the way the system works, in particular co-ordination?

Simon Constantine: On competition and consumer issues, there are areas where we are constantly looking to improve. In their Green Paper earlier this year, the Government identified that on the consumer side there may be better ways to enhance co-ordination. Those efforts are ongoing. Whether there are gaps that need to be filled by a new regulator is probably a separate question. Equally, Ofcom talked a lot about people such as the ICO. There is a degree of interaction between its remit and ours, and that is an area where we need to deepen relationships. We do some good work with the ICO already on specific cases, but more regular dialogue would be beneficial.

Dr Andrea Coscelli: There is a lot of ongoing co-ordination on matters. What worries me more now are potential gaps in the regulation as opposed to a lack of co-ordinating bodies.

Baroness Quin: Are you doing work on identifying gaps, or should government lead that work? I am trying to think where the responsibility lies for looking at gaps in the system.

Dr Andrea Coscelli: Strictly speaking, it probably sits more with government, but we interpret our remit in some areas as potentially trying to add value and thinking about those questions as well. For instance, in 2017, we spent a year looking at care homes as part of a market study. One of our key recommendations went across the regulatory set-up framework and the various responsibilities.

A month ago, this Committee asked us to look at digital advertising. That is something we are actively considering, subject to Brexit in the next few weeks, because it has a big resource implication for us. It is certainly something where we are interested in getting involved. If we did, we would work closely with Ofcom and give serious thought to the regulatory framework in that context.

Baroness Quin: Is there a regular mechanism whereby you can express your views on these issues to government?

Dr Andrea Coscelli: Yes. We have extensive discussions. On a matter such as this, we have discussions with the Department for Business, Energy and Industrial Strategy, DCMS and obviously Ofcom. For us, the extent to which this becomes public is usually linked more to a specific piece of work where we explicitly talk to stakeholders and publish something, so launching a market study would be the outcome. To give you an analogy, this morning we launched a market study on statutory audit. That piece of work is closely linked to initiatives brought by the sector regulator and the Government in a specific case linked to the Kingman review of the regulatory framework. Quite a lot of the work we do is linked to other initiatives because we find that is the best way for us to add value to the overall system.

Baroness Quin: If you make recommendations, on the whole do the Government follow them up? I ask this with some feeling, because committees make lots of recommendations to government and they are not always followed up. Sometimes they are.

Dr Andrea Coscelli: There is a mixed track record. As you know, recently there has been less domestic legislation going through Parliament. We think that some recommendations have essentially been accepted by government, but they are not part of a draft Bill yet, and hopefully they will become so. In other cases, we think we need to be involved post report to make sure that, as part of the implementation, the Government take it forward. In a sense we do not see our role as ending with the delivery of our report; it remains part of an ongoing discussion.

The Chairman: Dr Coscelli, thank you for telling us what you did about your consideration of the digital advertising market. Can we ask that you keep the Committee informed as your considerations progress?

Dr Andrea Coscelli: Yes, certainly.

The Chairman: As you know, it is an issue of interest to the Committee. Dr Coscelli, you are head of a powerful organisation. We have been talking about your relationship with the other regulators. Can you characterise the leadership relationship between you and your co-regulators? Do you meet on a regular basis? Is there a formal leadership forum where you discuss not just the immediate issues or the agenda of your organisations but perhaps the broader context in which you operate?

Dr Andrea Coscelli: Yes. We lead a UK competition network that meets two or three times a year. One of the sessions is explicitly a strategy session, a bit of a horizon-scanning session. All the economic regulators are part of it. We have quarterly senior-level meetings with the chairs and chief executives of the key economic regulators we work with. The vast majority of CMA projects in the past few years have involved at least a regulator of some sort.

As I was saying earlier, we have found that one of the best ways for us to add value and to diminish duplication is to work with other public sector agencies. In many ways, we do not have deep sectoral expertise, so it is very important for us to acquire that. There are often secondments of case teams and very frequent meetings. This happens at all levels of the organisation. Obviously, the leadership level is important to ensure that, culturally, there is the right environment for the teams to have those conversations. It is in a very good place, as has been recognised by others as well.

The Chairman: At leadership level you see yourselves as convenors, not just participants.

Dr Andrea Coscelli: Absolutely. It depends on the issues. There are some issues where naturally sector regulators feel they are in the lead. The way I think about it is that, if you are the leader of Ofcom or the FCA, you feel you are accountable for the outcomes in that particular sector. We feel that we are accountable for the outcomes across the piece, and for making sure that our competition and consumer powers are used when useful to achieve the outcomes. In that sense, it is a slightly different sense of accountability, but we work very closely to ensure we are all happy with the role we play.

Q137 **Viscount Colville of Culross:** I would like to ask you about the tools you can use to look at the abuse of market dominance. In paragraph 42 of your submission you say that questions are being increasingly asked about companies with strong competitive advantages being toppled by new, innovative entrants. You say that "certain businesses have acquired a commercial power which makes them immune to the competitive pressures which competition laws are designed to foster". Should you be looking to use tools in a different way, moving your focus from prices and consumers and switching to the behaviour of companies with investment and innovation?

Dr Andrea Coscelli: There is a very active debate, which to some extent resonates with some of the earlier discussions with Ofcom. In many ways, when I go to events in the United States and Germany, there are very similar discussions. The discussion is whether competition law can be interpreted in such a way that some of these new business realities can fit it and allow us to achieve the right outcomes, or whether there is a gap. I think the jury is out at the moment. Different people have different views on it.

Our current view is that the framework is quite flexible. We think that a lot of the business reality and changes can fit the framework and we can achieve the results we need. For me, the main risk, as we tried to put in the submission, is that business and economic reality can come into the assessment of cases quite easily and naturally, but, to the extent that you end up in litigation in a court-type process, the natural tendency in case law is to look at the evidence you have and to have a fairly high bar for evidence for competition authorities potentially to interfere with commercial operators. In markets where things change very quickly and there is a significant element of uncertainty, there might be a gap, and people are saying that maybe we need to change some of the frameworks. That is where the discussion is currently.

Baroness Kidron: It seems that in various areas, not just this one, there is a debate about harmonising laws. You make small moves to say that they apply, so that where you do not have case law you at least have the assertion that they now apply in these new environments, versus whole new laws that somehow seem to create a problem with different standards for online and offline. Is that part of the same discussion you are finding everywhere? Are there slightly smaller things one can do to tip the hat so that the courts can see it?

Simon Constantine: Going back to what Andrea was saying about our flexible framework, I think it is founded on the idea that it should be technology-neutral and should apply to both equally. Our principal message is that, on both the competition and consumer protection sides, online businesses are subject to the same laws as offline businesses. A number of the practices we see are very similar to the ones we have traditionally seen. Some of the challenges are, first, for us as regulators to understand those markets better—the expertise issues that have been discussed a lot today—and, secondly, the question of pace: the risk that by undertaking long and detailed evidence-based investigations, as we rightly do, with very fast-changing markets you end up remedying something that has already moved on.

Baroness Kidron: On case law, if that is a point of failure, that is something that government can speak to specifically.

Simon Constantine: Putting in ex ante rules to address it is one option. There are areas. With any kind of regulation, evidently the trick is to ensure that it is sufficiently well targeted and adaptable so that you do not end up inadvertently locking in the incumbent system.

Viscount Colville of Culross: You said in paragraph 47 that in a full competition enforcement investigation you can "impose time-limited interim measures to avoid significant harm", but you think that currently the powers are "subject to a number of legislative procedural requirements" which you would like to see changed. Can you go into that in further detail? What sort of changes would you like, and how would that benefit your ability to operate more effectively?

Dr Andrea Coscelli: It is interesting that the European Commission has similar issues. The issue is the balance between the rights of the parties under investigation versus third parties. If we receive a complaint from a business that feels it is being excluded by a larger rival, at the moment the process we have to follow under our interim measures process, which is the fast track to try to get a result more quickly, gives very significant rights to the business under investigation in terms of access to file and confidentiality. In practice, for us that means it is almost like running a standard case; the first track feels very close to the standard case.

When we are deciding what to do, we think that trying to run, essentially, two cases—a fast-track case, which feels very similar to the standard case, and then progressing the standard case—is not a very efficient way of doing it, so we end up just running the standard case, and the fast track becomes a tool that we very rarely use. That is what we would like to see changed, but it is for Parliament to decide the right balance. It is always difficult to take rights away from businesses. The reality is that, by not doing that, at times you take rights away from other businesses which are the complainants.

Viscount Colville of Culross: What are the changes you would like to see?

Dr Andrea Coscelli: It is very much about 'access to file' and the rights of defence for the business under investigation before we can achieve tangible results through interim measures.

Simon Constantine: A lot of balancing has to be done in considering the rights of both sides, and the decision we take at the end to impose interim measures is subject to appeal. Therefore, there is a risk that that is appealed, and it runs very much counter to the very intention. We are looking at how we might use interim measures and the level of proof you might need, and whether through the design of the interim measures you can reduce the risk of harm to the company on which you are imposing things, and the duration and extent of that, but the underlying requirement of the steps we have to go through makes it very difficult to ensure that—

Dr Andrea Coscelli: We talk about it because the French competition authority has successfully used interim measures in the digital space over the past few years. As regards the European debate, a number of agencies are in the same position we are in, where we find it difficult to use the measures. Looking at the French situation, we think they have achieved some results that we would have liked to achieve ourselves, so that is a prompt for ongoing discussions with government on this.

Q138 **Baroness Chisholm of Owlpen:** How do you ensure that the competition law assessments strike the right balance between short-term efficiencies and long-term innovation?

Dr Andrea Coscelli: That is something we do in every case. A consumer welfare test is very much focused on the future; it is about innovation and the way the market will be in the next few years. The difficulty, which is linked to my previous answer, is that it is easier to measure and to be precise about short-term effects than it is about long-term effects, particularly with these types of technologies and businesses. At times, a potential risk for us in defending our cases in court is that a lot of the focus is on measurement of the short-term effects, and less weight is put on some of the longer-term effects. We are aware of that and we are working on it, but it creates an element of risk.

Two years ago, we prohibited a merger that was the acquisition by the Intercontinental Exchange, a large US-based exchange company, of a competing European trading business. That had significant elements of long-term effects. The decision was challenged by the Intercontinental Exchange. We successfully defended it in court, so it is possible to do it in a way that allows us to get the right outcome.

Baroness Chisholm of Owlpen: Presumably, innovation is moving so quickly that no sooner are you working on one thing than it has already moved on to something new. It must be very difficult to keep up with the pace.

Dr Andrea Coscelli: Absolutely. To my mind, and I think a number of colleagues are in the same place, the international discussion of these issues up to a few years ago was almost that, given the pace of change and the complexity and uncertainty, it was very difficult to intervene in a successful way, so there was very limited intervention, as you know.

The debate has moved on. Current debate is very much about smart intervention, which could be a combination of ours and potentially the sort of targeted regulation Ofcom was talking about. Potentially, you can go all the way to a situation where very heavy regulation, such as public utility-type regulation, is needed, but I do not think that is where the majority of people are.

It is difficult, but it is not beyond us to think about the right forms of intervention. It is important to bear in mind that the mistakes need to be on both sides. Sometimes we make mistakes because we do not intervene when we should, but once in a while we might intervene when we should not. We have spent too many years working and thinking exclusively about mistakes on one side, and we need to rebalance that.

The Chairman: For clarity, the mistakes you have been focusing on are those of over-intervention.

Dr Andrea Coscelli: Yes. Generally, we have been in the same place as other leading agencies internationally in that we have been very worried about over-intervention, and now the debate needs to be more balanced.

Q139 **Baroness Kidron:** In a way, my question is a subsection of Viscount Colville's. Traditionally, you have looked at price and so on; now we have huge data monopolies and it is not about price. In our inquiry into advertising we started talking about data as currency, so it has a value and a price. Do you feel you have the tools to look at the big data monopolies to see whether they are fit for purpose? Is there an opportunity, is it a disaster, or is it something in between? Mainly, I am interested in whether you have the tools even to look properly.

Dr Andrea Coscelli: The short answer is that we believe we have the tools. Two cases of interest are the acquisition of LinkedIn by Microsoft and the acquisition of WhatsApp by Facebook. Both cases were looked at by the European Commission, not by us directly, but obviously we followed them closely. The view of the senior officials of the Commission was that the traditional framework allowed them to look at those concerns. If they feel that the acquisition of LinkedIn by Microsoft had created a degree of control over data that would have made it difficult for competitors to compete in the relevant markets, they felt they could have intervened.

The answer is yes, but it is something that needs to be monitored very closely, because there is a risk that a gap is created whereby, in a sense, we are forced into a test that is a bit too narrow for what could potentially happen in future in terms of acquiring data from different markets. Antitrust works very much on overlaps. When you are buying a competitor, the concern is that you may buy someone that is not a competitor today but could become one in the future, it is quite difficult to block that under antitrust law, unless there is clear evidence that there are plans to compete.

The question is whether there is a gap. For instance, recently we launched a research programme to look ex post at some of the merger decisions in the digital space. We looked directly at the acquisition of Instagram by Facebook, and the acquisition of Waze by Google. We are going to go back and look at them. The Federal Trade Commission in the United States is doing a similar programme, and we are working with it to do that in a joined-up way.

Baroness Kidron: When that piece of work is complete, I would be very interested in seeing it and the thinking behind it.

Dr Andrea Coscelli: Absolutely. A number of people have expressed an interest, so we will try to make it available.

Baroness Kidron: It is a core question for us all at this point. My other question is about portability. A lot of people feel quite disappointed about how that is going at the moment. If portability was going slightly better, the question of data monopoly would be somewhat less intense for those of us who take a slightly critical view. Do you see those two things as part of the same puzzle?

Simon Constantine: Yes; interoperability and standardisation certainly have a role to play. You have the broad right under the General Data Protection Regulation, but evidently it is a very broad right, and the implementation is important, as you say. We are in the very early stages of that. There is also a significant trust aspect, to ensure that data, if people are sharing it, is adequately protected. That provides the context.

Andrea mentioned the Open Banking remedies, after our banking market investigation, in which, effectively, we required all the banks to use standardised APIs—application programming interfaces—to ensure that new entrants can come in and create new products based on that data and that, with people's explicit consent, consumers could share their data among different providers. So you as a financial consumer could share your financial data and, based on that, have particular products recommended to you or tailored for you. In principle, therefore, consumers should be able to drive competition, which should reduce the costs of switching, because they can take their data from one place to another. As I said, it also reduces barriers to entry for new competitors, because you do not have the 'data moats', as they are known, that other people cannot get at.

We are thinking a lot about this at the moment, as are the Government as a whole. They have launched a smart data review. We are thinking about other sectors where portability might be used. In Australia, they have done some work on this, looking at the energy and mobile telephony markets. The focus is currently very much on the regulated sectors, but also on whether effective ways can be found to enable consumers safely to move their data around in a way they can trust and which protects the incentives of businesses to innovate. Obviously, if there is no incentive for somebody to gather data because they immediately have to share it with everybody else, you need to be careful about that. Equally, consumers should have control over who they give their data to and how it is used when they give it; they should be able to give that data to different people and use that to drive competition.

Baroness Kidron: I cannot work out whether that is a bit like rearranging the deckchairs while the ship—the data monopoly—is driving ahead. One thing we know and love about this environment is that it is all very convenient; it is always very convenient to do what the bigger players would like you to do rather than what you are, potentially, allowed to do. Do you feel that in our inquiry we should look more at the question of portability, or should we look a bit more to the data monoliths for answers?

Dr Andrea Coscelli: We are at a stage where portability is a good candidate for a lot of the heavy lifting in this area. We are certainly putting our time and effort into it, working closely with a number of other partners.

Q140 **Baroness McIntosh of Hudnall:** These questions are all roughly in the same territory. A moment ago, you mentioned public utility in respect of other kinds of consumer product. Do you think we are close to having to regard the internet and all its many iterations and uses as a public utility and, therefore, to be regulated in a similar way? I shall leave that one to stick to the wall, because you might want to respond or to think about it.

In particular, I wanted to ask about the existing tools you have in respect of offline activities and, in particular, the notion of a public interest test. The question of market dominance, which you have talked about at various points today, is clearly germane in respect of the big platforms, and invites questions about what is or is not in the public interest and whether you can apply tests.

What would be the risks and benefits of trying to apply public interest tests in this field, particularly given what you just said in response to Lady Kidron about the thinking you have already done about the mergers and acquisitions that have already happened? What conclusions did you come to? You said that you had looked at that, but you did not say what you had seen. Can you put that together and tell us where your thinking is going?

Dr Andrea Coscelli: Yes, we are doing it at the moment, but we have not reached a conclusion. That is why I did not mention conclusions. On mergers, there are three public interest categories. One is media plurality, which was used in the context of the Fox-Sky review; the second is national security; and the third is financial stability. Parliament could add a fourth category, say, the creation of data monopolies. There have been discussions in separate contexts about adding R&D as a further category. Whether to expand public interest in the review of mergers is an active debate, here and in a number of other countries.

There are pros and cons. The main counterargument is that you create a degree of uncertainty around foreign direct investment and the acquisition of companies. For the sake of argument, let us suppose that we end up with a public interest test on data monopolies. If you are a large platform and want to buy a small start-up, potentially you could worry that we might go against it on the basis of public interest. That is the downside.

The upside is that you give us greater flexibility to make a judgement.

At the moment, when we intervene on mergers, we have case law and the law on consumer welfare, so there is a fairly tried and tested methodology to look at it, which is reasonably flexible but has some limits. We could make a judgment that, right now, we are very worried about the accumulation of data for some of those platforms, so, ideally, we would like to block a particular acquisition, but our legal assessment might be that we cannot do so in the context of the law as it is. Adding public interest would allow us to do that, which could be the advantage of doing it.

Baroness McIntosh of Hudnall: Where other kinds of utility are concerned—water, electricity and all that sort of stuff—there is an anxiety, which is built into the way you regulate, that certain types of people are likely to be excluded from access because of the particular way they conduct themselves economically. Do you see any danger in future, as data becomes more and more the commodity that is traded, that classes or types of people will be excluded from areas of public discourse by the fact that they cannot participate as fully in the online world as other people? I do not mean that just in terms of conversation; I mean it more widely than that.

I ask that because, in a review of a book I have been reading, I have just read about a scheme already under way in China that gives citizens a trust score based on their communication and purchasing behaviour. If you have a low score, says the reviewer, you might not be able to book a train ticket. Obviously, that is not where we are; it is thinking a bit ahead. Do you foresee any danger of that kind of exclusion growing out of these datasets?

Dr Andrea Coscelli: That is something to think about and, potentially, to worry about. It is firmly in the remit of potential regulation. There are a number of sectors, such as energy, water and telecoms, where regulation has been firmly established for a number of years, and the regulators have specific duties on exclusion, vulnerable consumers and various other considerations. There is a scenario whereby we could end up with a portion of the internet that is regarded in a similar way, and regulated in a similar way. A few weeks ago, there was a report by the

IPPR that was regulatory in the nature of its recommendations for the internet.

At the moment, we and a number of our sister agencies internationally are in a more intermediate space, where we think that it is probably better to focus on some aspects of regulation and still hope that innovation, competition and the potential leapfrogging from one model to another will generate a lot of benefits for consumers. From regulating networks, we know that it is a bit of a plan B; it is not ideal. It is the best we can do, but there is a lot of time and effort on generating the outcomes. Before we develop a heavy regulatory framework for the internet, we would probably want to see more evidence that there are more enduring and entrenched problems.

Simon Constantine: We have been looking a lot at the remedies we impose: things such as data portability, competition-focused remedies, and efforts to make people switch their bank or energy accounts more. Those are very much competition-driven remedies, and for some people they will work. People who are unable to engage in a market, or do not engage, may not benefit. We are looking at our remedies and asking whether the balance is right for the active consumers we want to encourage to switch, because ultimately that is what drives competition and innovation, and the people who might not be able to benefit from that. Within those, you want to select the generally vulnerable, who are unable for whatever reason to engage in markets, and think about how to address that. Some of it may come in the way we design our remedies, but, as Andrea says, you may find that that is where you need a degree of more direct intervention.

Baroness McIntosh of Hudnall: The world is moving to a situation where more and more of people’s life is conducted online—for example, access to healthcare—which is generally seen to be a positive in some respects; but there is no question that for some people, if that becomes the dominant method of delivery, it is not a positive. It is particularly not a positive if the delivery mechanisms are dominated by two or three major platforms as the means by which things are made available. I do not want to put words into your month, but, given that that is how things are going, I sense that you are saying, “Yes, it’s sort of a problem, but we’re not really sure that it is much of a problem yet”.

Dr Andrea Coscelli: We are absolutely focused on the experience and outcomes for consumers. The question is about the best way to get there. With healthcare, for instance, there is a sector regulator, NHS Improvement, which might have a role in regulating some of the digital providers in the healthcare space. We have consumer protection, which is essentially regulation, so there are a number of things they have to do anyway. There is always a degree of regulation; the question is whether you need extra layers to achieve what you think you need to achieve.

We completely share your view that what is needed is that the outcome for consumers in a particular situation is the right one. I do not know about the specifics in that particular case, or whether we might think that other providers might provide a similar product, and that giving them access to the data through our data portability remedy might be the best way. To have four platforms innovating and competing is better than having a heavily regulated single platform. It would be a case-specific assessment. In theory, I completely agree with you. It is just about the specific application and what's the best way of getting there.

Q141 **Baroness Bertin:** I shall keep this brief and make it quite simple in the interests of time. If you were to change one thing about the current law to make your job more effective, particularly with regard to the online economy, what would it be?

Dr Andrea Coscelli: That is a good question. The point about interim measures is important. The second area is consumer protection law. We have asked for better powers from government in the last couple of years. For us, one key area for consumer protection is fining powers; for instance, when we intervene against a number of providers in the online gambling or dating space, we cannot penalise the operators who are materially in the wrong place as regards their compliance. As one of their lawyers said to me, at the moment there is no business case for compliance. Essentially, they drag their feet and resist us, and, eventually, they end up doing the right thing, which they should have done 18 months before.

The Government have agreed and have said that, when there is room for legislation, they will give us fining powers. Linked to that, the current model is one whereby we have to go to court, as in the case of viagogo, a ticket reselling website. We would like the same powers as we have on the competition side, so that we can take decisions ourselves and potentially fine a company and get remedies. That is what a number of other agencies in Europe and internationally do, and they are quite effective in doing it. If we brought consumer power into a similar sphere to competition power, particularly for digital, the two sets of powers would be complementary and would allow us to achieve a lot.

Baroness Bertin: Do you think that existing legislation could be tweaked to get you that, or would a wider Bill have to go through?

Dr Andrea Coscelli: We think that for consumer power it would have to be primary legislation, so it would have to be part of another Bill.

Q142 **Baroness Kidron:** My question is about consumer protection, specifically on terms and conditions. Is it not a regulatory failure that we rely on terms and conditions, and that 99.8% of people tick them and never read them, period? That is my first question. When you have answered that in short form, I also want to ask whether you would extend it to other things, such as using consumers' emotional states to create a decision, or persuasive design. It might be connected with your report, where you raised the question of whether terms and conditions should inform consumers if there was personalised pricing. It could be like drug companies having to tell consumers about side-effects. Can we rely on terms and conditions, or is there regulatory failure? What should be in them, and should we be more demanding about what is in them?

Simon Constantine: On your first question, it is one of the incredibly intractable challenges. We have all experienced it personally. How do you get all the key information in front of consumers that they need, get them to read and understand it and enable them to have some kind of meaningful choice at the end? If you get a breakdown in any of those points, you have an issue, because you end up with a situation where either it is not read or it is not understood, or it is read and understood, but people feel that they have to click through anyway as a result. That again is something we are looking at, whether it is a combination of specific rules or principles, or certain nudges that you can make to get the right information in front of the consumer. Certain things have been tried, such as cookie notices, although I think we can all say that they may not necessarily have worked as they might.

A lot of experimentation is going on in government and internationally about how we can get terms and conditions to be more effective in doing what they are supposed to do, which is to make consumers aware of what will happen to their data—what has been gathered and whether it will be sold—and to give them a choice. If they have a choice, we hope that will create incentives for other people to offer better terms and conditions, creating a degree of competition, which we do not really have at the moment. People do not go from one product to the next, reading through all the terms and conditions and comparing them. You cannot have that perfectly, but there must be elements where people can promote themselves on the various terms they offer.

More generally, consumer protection law has an important role. As Andrea said, one reason why we are keen to bolster our powers is that the underlying laws are potentially very effective in this area. It is about looking at unfair terms in and of themselves, which applies equally to online platforms. If people are insufficiently transparent about data they are gathering or how it is used, that can potentially be unfair and unenforceable.

There are also certain misleading commercial practices. Some of the practices intended to exploit biases and to rush people into making decisions may be unlawful. One of our concerns with some of the sites that we have looked at recently is the ticker across a site that turns out to be meaningless but is designed to create a sense of time pressure or scarcity. And with our hotel investigation, we are looking at whether some of the scarcity messages might be misleading by inducing customers in that sense. The laws are there, and we are looking to see how best we can use them, and we feel that additional enforcement powers will create a strong sense of deterrence at the outset.

Baroness Kidron: Can I press you on this point? I know that you are doing very good work in this area, looking at comparison sites and other things. If we all roll our eyes and say that we do not read them, or that they do not offer a choice, do you have the right laws? I am very sympathetic to the enforcement bit, and I understand exactly the point—noted—but the system is not fit for purpose. It is not just the end bit or the enforcement bit; there must be something wrong up front.

Dr Andrea Coscelli: That is where the ex ante regulation will come in, in my view. Ex post enforcement works well with enough ex ante regulation. When there are gaps in ex ante regulation, somehow we feel we have to do much more to compensate for it, and sometimes the tools are not exactly what you would use. For instance, with terms and conditions it would be much more efficient to have a degree of ex ante regulation, rather than us looking individually at specific companies or specific sectors without fining powers, just one by one trying to get people to the right place, which is possible but not the best use of our resources.

Simon Constantine: The ex ante thing has been done fairly well in certain regulated sectors. There are key facts documents, and other things, for various financial products, which work quite effectively. As Andrea said at the outset, we are looking economy-wide, and it becomes somewhat more difficult to work out how to create a standard that works for all those things, or to set a framework within which there is flexibility for each industry to create a series of mechanisms to get the right information to consumers, and then for consumers to engage with it.

The Chairman: It is a very interesting area.

Baroness Kidron: It really is.

The Chairman: What might it look like if you created a framework for terms and conditions to be agreed sector by sector? Would there be protection for businesses, if you identified the issues that in your view were most important to consumers and must be covered in the terms and conditions and on which there must be clarity—hence, keeping them short—while other things need not be terms and conditions and might just be a statement elsewhere on the company website? As well as an enforcement role, would you see it as having protection for businesses to enable them to keep their terms and conditions short and to the point?

Simon Constantine: Trying to work out which are the key terms is clearly important. Experiments have been done about whether you can create some kind of 'trust score', a fairness rating or something like that, for terms and conditions, or whether to have a kind of cascade system where certain terms are prominent, with click-throughs and so on. A lot of that behavioural research is being done in other countries, from what I have heard, and similar research has been done here. Shifting consumer behaviour is very difficult, but that should not stop us trying.

If we are looking at a particular market and asking how we can make competition work well in that market, these sorts of issues arise: how to get the right sort of information in a motor insurance or banking market and what sort of information consumers need. We have league tables in banking, for which you will have seen the adverts; some banks are making quite a lot about the fact that they have come top of our tables for that. There are all those different ways, and it is just about designing the right one. As we keep testing those sorts of remedies, I hope we can become better and better at it.

The Chairman: Thank you both very much. I am very interested in the evidence you have given, and I know that the Committee is, particularly the perception that public opinion is changing internationally and nationally, and consequently the remedies you are putting forward will change accordingly. The points about gaps in the regulatory powers and the co-ordination with other regulators are very interesting, too. I appreciate that you have a very broad remit and that you have clearly kept abreast of the work of the Committee in this important area.

Dr Coscelli, is there anything we might have asked that we have not asked, or any other points that might be useful for us in coming to our conclusions?

Dr Andrea Coscelli: No, we have covered the main issues that we wanted to talk about.

The Chairman: In that case, thank you very much. As we develop our report, we may come back to you with technical questions and ask whether you can direct us deeper into your organisation to someone who can help us. Thank you very much for your time.

Cybersalon – written evidence (IRN0030)

1. The Open Web and the closed platform

1.1 There is a clear distinction to be made when we speak of the internet. On the one hand, proprietary platforms[686] and the ecosystems which surround them, the walled gardens of Facebook, Instagram, Amazon, and on the other the open web, a tapestry based on open standards, Wikimedia, Creative Commons, the Mozilla Foundation and the software and protocols that form the foundations of the World Wide Web. Whilst the wider discussion is chiefly concerned with dealing with problems caused by undesirable content and behaviour on social platforms, lawmakers should be very careful not to place undue restriction on the open web, the open standards and infrastructure of the digital economy and culture that we so value and take for granted now.

1.2 The internet is a panoply of networks, built upon shared protocols that form the basis and foundation for websites and digital services to operate from. Facebook, Google, Amazon, Apple use but are not part of the Open Web, nor do they embody the internet, they may be regulated as online-based digital examples of existing businesses ranging from broadcasting and advertising to retail. We need not enshrine new precedents and categorisations in legislation that leads to unexpected loopholes and unintended consequences.

2. The extension of fundamental rights into the digital age

2.1 This submission is predicated on an understanding of the successive development of rights and freedoms, that the new digital age, defined by an ever increasing role of the internet and digital platforms in our lives, warrants a new debate over how to construct a new constitutional settlement which nurtures today's emerging forms of digital citizenship.

2.2 Fundamental rights laid down in the 17th and 18th century liberal formulations of political and civil freedom were grounded in widespread economic exploitation. Such fundamental rights, in practice, were often the privilege of the few. At our current impasse we risk a similar submission to power in this new digital age, from the rise of the phenomenon of platform dominance from the likes of Facebook and Google who now play a key role in mediating the civic, political and economic life of the nation and the world[687].

2.3 The following pages detail a set of recommendations that constructively and proactively set out the case for user rights, in opposition to the current state of platform dominance.

3. GDPR is good, but Britain can do better

[686] Open Web - Wikipedia https://en.wikipedia.org/wiki/Open_Web

[687] Digital Citizenship: from liberal privilege to democratic emancipation, OpenDemocracy https://www.opendemocracy.net/richard-barbrook/digital-citizenship-from-liberal-privilege-to-democratic-emancipation

3.1 GDPR as an EU Regulation will apply unilaterally across the EU, but it does contain provisions for member states to expand and withdraw from the Regulation in certain ways. Germany has already legislated with the Federal Data Protection Act. The UK can follow suit, acting to close loopholes present in the legislation such as the 'escape' of data outside of the EU for example by handing over personal data via transactions to non-EU organisations without adequate protections, the loss of GDPR protections by non-EU organisations selling data to third parties not related to the offering of goods and services and so on. These are just an example of where the UK can improve upon and enhance existing legislation.

3.2 Fundamentally, GDPR leaves too many opportunities for data leakage. Users must have confidence in the overlapping systems, policy instruments and legislation that are purported to protect their online privacy and personal data when using the internet. As we presume innocence until proven guilty, we must presume that the user has the right of control and use over his or her data.

4. Curatorial versus editorial control

4.1 Algorithms are merely rules and processes. They are designed by humans, composed of human decisions, and in the case of platforms, human decisions informed by corporate goals and directives. Facebook and other major platforms hide behind the obfuscation that their platforms and the content served on their platforms is automated, that it is presenting posts and inputs as they are submitted to the platform. This is not the case.

4.2 Let us be clear, they are not just curating our social experiences, but rather taking on an editorial role. Take the example of Facebook's recent alteration governing which content from which sources are served to the user's newsfeed, the Facebook timeline. This change altered the distribution of content on the news feed weighting in favour of posts and media from friends and family over organisations and companies. Facebook and other social networks are presenting a very specific view of the world; they are mediating and filtering engagement in the online space. They have taken on the role of the editor, but claim they are merely re-presenting inputs, a curatorial role.

4.3 Facebook, Twitter, Instagram and others are closer to that of online magazines, where the magazine is edited by a team of editors; the Facebook newsfeed is edited by algorithms, rules and if-statements, developed by humans, reflecting human goals. Facebook's own Community Standards are an example of hands-on editorial control[688]. As a result they should be held accountable under existing laws as would any other publisher for the content therein.

5. Algorithm accountability and access

5.1 Software and computer code are often put into escrow when commercial suppliers need reassurance that software a buyer commissions will still be usable

[688] Community Standards, Facebook https://www.facebook.com/communitystandards/

if the supplier fails financially[689]. Alternatively, information and patents are held in escrow, set aside whilst competing parties vie for their claims. We argue a similar instrument can be used by Parliament or a new monitoring body to provide access to platform code and algorithms for researchers to examine.

5.2 Such instruments and monitoring bodies with access to the algorithms of platforms allow Parliament and civil society, under certain conditions, to gain an understanding of the intentions and aims of platforms and their use of data, including socio-economic goals. Parliament cannot legislate effectively, cannot scrutinise effectively what it does not understand. As a result policy responses in this sphere have largely been reactive rather than proactive based on an educated evidence-based approach. Given the monopolistic nature of these companies that govern and harvest the daily activities of billions of people, such an approach is not unwarranted given the current threat of their activity further undermining the established supremacy of Parliament and the democratic process.

6. The case for moderation

6.1 We often think of the internet as a self-managed community, and by extension expect online moderators to work for free. This has come from the historical fact that the original online forums such as Usenet were specifically not-for-profit. Moderators then were part of a self-governing community of non-commercial groups. In other cases commercial services such as AOL offered free use of their service in exchange for moderation.

6.2 Facebook, Twitter and the platforms are commercial entities, earning millions leveraging user content. Facebook does not have services it can provide in kind, except the use of its platform without processing the user's data. It should employ moderators and pay them. In addition to this, lawmakers should bear in mind the kind of content moderators are obliged to expose themselves to, from child pornography to extreme gore and hate crimes, and factor this into their decisions.

6.3 As things stand, social platforms are left to exercise their own judgement when it comes to taking down offensive content. We back the view of the Independent Committee on Standards in Public Life with regard to their recommendation to shift the liability for illegal content onto social media firms. We add that platforms should be forced to remove offensive content within legally defined time limits and recommend the Santa Clara principles of moderation[690].

7. Social Network Ombudsman

7.1 "Free" platforms are not covered by existing UK ombudsmen. Ombudsman services are available only in cases where money is paid or financial transactions take place for goods and services. Users of social networks are consumers of the

[689] Software Escrow, SBA Research https://www.sba-research.org/research/projects/software-escrow/

[690] Santa Clara Principles, Digital Social Contract https://digitalsocialcontract.net/what-proportion-of-social-media-posts-get-moderated-and-why-db54bf8b2d4a

services of the social platforms and they pay for the "free" service with their data. However, because this is a non-financial transaction, social users have no recourse to dispute and complaint resolution when their user rights, or consumer rights, are challenged.

7.2 Alternatively, existing ombudsmen such as CISAS need to reframe their definition of "consumer" to include users who trade their data for services, such as Facebook, Twitter etc. This is important to state, given that the user relationship with platforms can be read as a supplier relationship. Facebook makes approximately £15 per user in the UK per year. Accordingly, users need a supplier contract and supplier protection.

8. Digital Citizens Advice Bureau

8.1 As it stands, despite internet usage now extending to above 80% of the UK population, internet users have no dedicated advice services. We recommend Parliament consider the establishment of a new internet user rights service, providing assistance and expert advice to British internet users regarding their online rights, privacy concerns and advice with how best to secure their online presence, similar to Childline. This would be particularly valuable internet users, both young and old.

9. Platform users have rights to their own content and remuneration

9.1 The content individuals post and share via online platforms belongs to them. We suggest Parliament consider the licensing of user content under Creative Commons. If content is used by the platform, such a scheme could include negotiated pay percentages based on usage data by the platform. Platforms economic value are predicated on the exploitation of colossal amounts and flows of individual's personal data and content.

10. Russia, China and the right to interrogate foreign company use of user data

10.1 Recital 23 of the General Data Protection Regulation provides a loophole, through the specific wording of *"offering goods and services",* allowing for foreign companies to 'escape' data out of the EU area by the means of marketing, rather than the selling of products. Put simply, a global company wanting to exploit this loophole and extract personal data belonging to British and EU citizens can set up a marketing company in the EU presenting a range of products and services, before taking the EU customer to a non-EU payments portal, transferring payment and personal data to a non-EU business. From that point on the personal data are "outside the law" and there are no barriers to the UK/EU citizen's personal data being sold on to any other non-EU company.

10.2 It is within the purview of Parliament to lobby the CJEU to rule that Recital 23 is a misinterpretation of EU law, and that "offering" should have the same interpretation as applied in competition law.

11. Combating shadow profiling

11.1 Facebook is understood to have built up profiles of non-Facebook users. Information about non-Facebook users is captured or inferred from the information posted to Facebook by their family and friends: they may be included in photographs, and their lives and jobs may be discussed in postings. The photos may also be passed through facial recognition algorithms. All of this happens even though they have not granted Facebook their consent.

11.2 This is possible and alarming because of the limited number of data points required to identify someone. Countless non-users are swept up and their data stored and used by the company, through simple acts of a new user uploading their phone contacts into Facebook to search for new friends through Facebook's People You May Know service. This extends to Facebook's Like and Share buttons on websites external to Facebook; these all track non-users through the internet, building up a Shadow Profile.

11.3 When users ask Facebook to delete their account, they expect the company to delete the information they have uploaded since their profile was created. However, the information Facebook has inferred and collected about them, for example, from their activities on the web - that is, their Shadow Profile - remains on Facebook's servers. When we talk about scrutiny of algorithms, algorithm escrow and the consideration of new forms of monitoring to better understand these systems, we are arguing that policy makers must educate themselves about precisely this kind of activity by internet platforms.

12. Risks and capacity of current oversight

12.1 The Information Commissioner's Office has limited capacity with only 500 full time staff to oversee 500,000 companies that hold data and operate within the UK, the enforcement of FOI & GDPR rules, and for the 40,000,000 social network users. The ICO requires higher funding in line with the expansion of its portfolio of activities.

13. Unintended consequences

13.1 In the past when legislation has been written on the hoof, and without proper due diligence it has had unintended consequences. To cite two examples, FOSTA/SESTA, the anti-trafficking law in the US has effectively ended the rule of Safe Harbor, Section 230 of the 1996 Communications Decency Act[691]. The Computer Misuse Act has paradoxically made it difficult for security researchers to undertake their work in case of being implicated for the things they're working to prevent.

14. Conclusions

14.1 The new power of Facebook and Google is here to stay and is increasing. These new services and economies have brought about wonders, connecting the globe, empowering billions, providing next-generation services, toppling dictators, highlighting abhorrent behaviour with #metoo. But these new

[691] A new law intended to curb sex trafficking threatens the future of the internet as we know it https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom

platforms also come with new costs and threats, to our democratic process via paid Russian Facebook trolls, the political polarisation of global populations, the weaponization of personal data via Cambridge Analytica, the shaping of moods of entire populations via algorithms, a new torrent of unchecked hate crimes, a new generation of children socialised through the less than safe space of social media and YouTube, and the rise of hitherto untouchable economic monopolies based on the mass exploitation of personal data.

14.2 The current generation of platforms are companies that have been allowed to grow to monopoly status due to watered-down US anti-trust laws. Facebook owns Whatsapp, Instagram, Oculus and Messenger, an entire ecosystem that their users largely think are separate distinct entities. The size of the platforms matter. They affect millions of users, making them dangerous, and by and large, they are unchecked by regulation.

14.3 Because of their size, with a few dominant players, governments regulate these companies through conversations and backroom chats with a handful of corporate representatives, rather than legislating and making arguments publicly. The UK Government is not immune from this.

14.4 The approach of collaborating via the back door is not working, and as a result there are areas where the law is silent because platform giants won’t collaborate and they refuse to engage. Mark Zuckerberg’s recent refusal to speak to Parliament is a case in point. The government won’t take a stronger line for fear of being shut out.

14.5 The supremacy of Parliament itself is under threat, an issue that will be exacerbated when, post-Brexit, the UK will be attempting to regulate or mediate platform monopolies from a national level rather than a pan-European one. This point is worth the House's consideration. Zuckerberg has already refused to answer the UK Parliament's call to testify - yet he felt obliged to speak in person to the European Parliament.

14.6 Democracy requires open public policy discussions rather than private discussions based on relationships with powerful companies that take place behind closed doors. We believe Parliament should reassert its sovereignty. The current system of regulating these companies is not compatible with the public interest. In our view, the UK needs a Digital Bill of Rights to consolidate the progress of GDPR and cement user rights in law[692].

11 May 2018

[692] Digital Bill of Rights, Cybersalon.org http://cybersalon.org/digital-bill-of-rights-uk/

Digital UK – written evidence (IRN0062)

1. Overview

1.1 Digital UK welcomes the opportunity to respond to this inquiry on the future regulation of the internet. Our key points are:

- Freeview and Freeview Play provide a safe and trusted way for consumers to access high-quality online video content.

- Freeview Play secures prominence for UK public service programming through partnerships with global TV manufacturers, in a way that other online platforms do not.

- Freeview Play provides accurate and impartial news sources, at a time of heightened concern over trust in the online space.

2. About Digital UK

2.1 Digital UK supports the UK's terrestrial TV service and its viewers. The company is owned by the BBC, ITV, Channel 4 and Arqiva, the network operator.

2.2 We are responsible for day-to-day operational management and lead on development of the Freeview service, working with our broadcast partners and industry. Our goal is to create the best free TV service available to viewers, both live and on-demand.

2.3 Digital UK also works in conjunction with its sister organisation, Freeview, to provide viewers with information and advice about terrestrial TV channels, services and reception. In October 2015, Digital UK and Freeview launched 'Freeview Play', a new connected TV service.

2.4 Digital Terrestrial Television (DTT) is the UK's most widely used TV platform. Freeview is the main service on DTT - universally available and offering a range of more than a hundred free-to-air TV, radio and text-based services. It is watched in more than 19 million homes, or 7 in 10 TV homes. Freeview is the sole television service in more than 9 million homes[693].

3. About Freeview Play

3.1. Freeview Play seamlessly integrates live broadcast TV with catch-up and on-demand content and is free from any monthly subscription. Built into TVs and set top boxes it is an easy, accessible and affordable way to access PSB catch-up services such as BBC iPlayer, ITV Hub, All4 and

[693] BARB Establishment Survey Q1 2018

Demand 5. Content that was previously broadcast live can be accessed on-demand via the PSB player apps directly, via a scrolling backwards EPG (Electronic Programme Guide) or straight from the linear programme guide at Channel 100.

- Freeview Play has been adopted by 19 of the top 20 leading TV manufacturers, including LG, Sony and Panasonic, making it the most widely adopted on-demand platform by manufacturers.

- It is widely available through retail at a range of price points, starting at under £100 for a set top box.

- There have been over 3.5m sales of Freeview Play devices since launch in October 2015.

- Almost two-thirds of smart HD TV sales are now Freeview Play694

- The Freeview Play home-screen or 'user interface', is designed to secure prominence for UK PSBs through partnership with global TV manufacturers.

4. Response to the consultation

4.1 Overview

4.1.1 While terrestrial television has traditionally provided a secure, trusted and resilient means of viewing, the trend today is towards more viewing taking place online. Given that linear broadcast content is highly regulated and online content less so, this trend also means that viewers are increasingly moving between environments in which very different rules apply – often without necessarily realizing. Freeview Play is an example of how TV content can be aggregated and delivered over the internet in a way which guarantees viewers easy access to high-quality content they can trust.

4.1.2 The internet has dramatically reduced the barriers to entering the broadcasting ecosystem. There is now a proliferation of film and television content aggregators, ranging from those using platform functionality and features as a way of selling devices (Apple TV, TV manufacturers, mobile device companies), a model using a blend of functionality, differentiated content and wide distribution to maximise subscriptions (Netflix, Amazon Prime) or user engagement with advertising-funded content (Facebook, YouTube).

4.1.3 Connected televisions and OTT services are also growing exponentially, driven by consumer appetite for a single access point to linear and on demand content. 80% of TV sales are now smart TVs[695] and ten million

[694] 59% - GfK data for Jan-Mar 2018

[695] GfK Panelmarket, volume sales, Q1 2018

homes have a subscription to an OTT service such as Netflix, Amazon Prime or Now TV[696].

4.1.4 Global players are making the television screen an increasingly competitive place and use their power to buy prominence at the expense of UK broadcasters. This can make the viewing experience for the consumer more confused, adding numerous layers of overlapping services.

4.2 A regulated and safe platform

4.2.1 As the ways in which to access content proliferate – via both hardware (devices) and software (apps) – it is becoming more important than ever to have trusted and well-regulated entry points for entertainment services that can be accessed by all the family. Freeview Play provides a safe route to achieve this. Freeview itself is a product of industry coordination and commitment. This commitment results in a strong brand identity which is valued and trusted by viewers, with fully regulated and trusted public service content. Freeview Play now twins this with the extended choice and functionality which internet television can bring.

4.2.2 Freeview Play also brings with it accurate and impartial news sources. Ofcom's latest report into news consumption in the UK[697] was clear that broadcast TV is still the most popular way to access news and remains the most trusted source by consumers. Freeview and Freeview Play are home to BBC, ITV, Channel 4 and other commercial news services which are all regulated for accuracy and impartiality by Ofcom. This is in contrast to other online news services which may not be regulated, but are now also available on the main TV in the family living room through the internet.

4.3 Public service broadcasting prominence

4.3.1 The growing proliferation of platforms and interfaces is beginning to dilute the hitherto dominant role of the Electronic Programme Guide (EPG) which is subject to regulation to preserve prominence for PSB content. Global platforms, although currently carrying PSB broadcasters' apps in relatively prominent positions on their guides, may not promote the full breadth of UK PSB content, and attribution of programmes to the broadcaster may be limited. Newer platforms curate their content in very different ways, and have diluted the traditional way of discovering content. The same can also be true of more traditional TV platforms when delivering content over the internet and PSB prominence can be lost.

4.3.2 Freeview and Freeview Play remains a PSB-prominent interface, and sets new standards for what PSB-supportive discovery means online. This is

[696] BARB Establishment Survey, Q4 2017

[697] https://www.ofcom.org.uk/__data/assets/pdf_file/0016/103570/news-consumption-uk-2016.pdf

especially true on Freeview Play, given the platform aggregates both on demand content as well as linear channel programming. It does so by working closely with global manufacturers to achieve as prominent a position as possible for PSB channels and content within the context of other commercial negotiations.

4.3.3 Public service programming is highly valued by the British public and plays a critical role in the global success and economic contribution of the UK's creative industries. As access to TV content over the internet increases and more viewing takes place online, a supportive policy environment will be imperative to ensuring public service content continues to be easily found and consumed by UK audiences.

May 2018

Doteveryone – written evidence (IRN0028)

Introduction

1. Doteveryone is a think tank that champions responsible technology for the good of everyone in society.

2. The findings of our People, Power and Technology research[698] into the public's digital attitudes and understanding show people are concerned about the impacts of the internet on society, feel disempowered in the face of technologies and have a strong appetite for greater accountability from technology companies and government.

3. In our People, Power and Technology report we called for independent regulation and accountability, so standards are upheld and people know who to turn to when things go wrong. We are developing this idea further in a forthcoming Green Paper which makes the case for a new regulatory body, that understands the complexities of the internet and can develop new thinking for regulating in a fast-moving digital world.

4. This written evidence presents the key findings of this work and complements the oral evidence given to the Committee by our CEO Rachel Coldicutt on 8 May 2018.

1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

5. Public mistrust of technology companies is high, with 43% saying there is no point reading terms and conditions because companies do what they want anyway. Two-thirds of respondents feel that government should be responsible for enforcing digital companies to treat their customers, staff and society fairly, but only 36% agree that government is currently able to address the problems they have with the internet.

6. The key problems we identify in reviewing the current regulatory landscape for digital technologies in the UK are:

   - Regulators adopt a reactive approach to digital issues, which can mean accountability comes too late and is more difficult to enforce.
   - Regulation focuses on outcomes, which means the processes and design of technology is under-scrutinised.
   - A tendency to focus on individual rights and issues such as safety, data use and security also crowds out concern for social impacts, such as technology addiction and algorithmic discrimination, that are only visible when assessing the effect of technologies across large groups of users.
   - The current status quo of siloed regulators focusing on bounded sectoral impacts means emerging cross-sectoral issues such as the

[698] http://understanding.doteveryone.org.uk/

internet of things routinely fail to be addressed. Collaboration between regulators does occur but is ad hoc and still leaves many gaps in regulating digital technologies.
- The public's awareness of ways to gain redress for breaches of their digital rights and a lack of mechanisms for collective redress mean that digital technologies are not effectively being held to account for their impacts on society.

7. We believe regulating a complex fast-moving digital world requires a "systems approach". This approach recognises that government, industry, civil society, technology users and the public all have a role to play in defining an internet that works for the good of society. In this context an independent regulatory body is vital to bring these groups together and develop mechanisms to hold them all accountable. We believe this independent body is needed to:

- Build up industry-standard expertise to scrutinise the underlying technical structures of digital technologies, auditing design processes, conducting independent impact assessments at an early stage of a technology's lifecycle and developing industry standards for responsible technology design.
- Lead horizon scanning and foresight activities to identify emerging digital issues and conduct studies to develop an evidence-base around issues whose impact is seen on a societal level.
- Advise current sectoral regulators on emerging technical challenges and co-ordinate unified responses for cross-sectoral issues Convene stakeholders to develop a collective long-term vision for an internet that works for the good of society, running deep public consultations and working with industry, civil society and government to understand how ethical frameworks can be applied in a messy real-world environment.
- Build up public understanding of digital issues so that society is able to use these regulatory levers for accountability effectively, providing mechanisms for technology users to raise concerns

2. What should the legal liability of online platforms be for the content that they host?

8. This question reflects the current focus of public debate around how technology companies are classified and specifically around how content on social media is regulated. However Doteveryone stresses that regulation must include but also look beyond content regulation and favours the development of a holistic approach which will help foster responsible technology.

9. Many online platforms offer a range of cross-sectoral services, and attempts to legally define them (for example as publishers, or utilities) are over-simplistic and contentious, as the objection to Article 13 of the EU Copyright Directive[699] shows.

[699] http://www.create.ac.uk/blog/2018/04/26/eu_copyright_directive_is_failing/

10. Using blunt regulation that places full liability onto platforms is problematic as platforms may over-regulate legitimate content in efforts to negate any risk of liability - This has serious implications for freedom of expression. "Voluntary" approaches where platforms police their own content are equally problematic, as they are not qualified to distinguish legality from illegality online. Platforms self-policing legal harms, lack democratic legitimacy as there is little opportunity for the public, civil society and government to have their say on what constitutes a "harm", and where the damage caused by it outweighs the right to freedom of expression.

11. William Perrin, a former civil servant with experience setting up regulators, offered an alternative approach during our own consultation by using the principles of "duty of care" and harm reduction that are commonplace in many other sectors such as medicine and employment. Under this approach, platforms and service providers would be obliged to prevent users from harm and demonstrate the steps they are taking to do so. A regulator could then map all issues arising from a service, develop plans to address them and share good practice with other organisations working in a similar space to prevent problematic practices spreading across the industry. In placing a proactive obligation on companies, they are encouraged to innovate to tackle issues head-on.
12. The 'precautionary principle' used commonly in environmental sectors offers another legal precedent in this area. This principle is applied in situations where there are reasonable grounds for concern that an activity is causing harm, but the scale and risk of these issues is unproven. The onus is then on organisations to prove that their practices are safe to a reasonable level. In the UK, the Environment Agency has the power to enforce 'stop notices' that require organisations to halt activities until they have been proven to be safe. Applying this thinking to internet regulation, technology companies could be forced to stop or alter practices that preliminary evidence suggests cause harm until an independent auditor has assessed their impact and stakeholders have been consulted. Taking algorithmic discrimination as an example, organisations could be required to halt their use until they have been tested for bias[700].

6. What information should online platforms provide to users about the use of their personal data?

13. Our research shows people care deeply about the use of their personal information - 95% say it's important to know their data is secure, 94% say it's important to know how their data is used. And they would like more control over it — 91% say it's important to be able to choose how much data they share with companies, but half (51%) can't currently find out that information. We found that people have little understanding of how companies collect data about them.

[700] https://www.newscientist.com/article/mg23431195-300-bias-test-to-prevent-algorithms-discriminating-unfairly/

14. While around a third don't realise that information about previous searches or purchases is collected, two-thirds are unaware that information about their internet connection is gathered and over 80% don't realise that information which other people share about them is collected[701].

15. The information which platforms currently provide clearly does not help people to understand how their data is used. 89% want clearer terms and conditions[702], whilst previous research suggests reading the privacy policies for all online services used would take between 10[703] to 25[704] days per year for the average person.

16. Providing users with more information, whilst well intentioned, is unlikely to give the public more control over the use of their online platforms. Ensuring online platforms go beyond transparency to making their services understandable (for example by developing common standards for terms and conditions) should therefore be a regulatory priority. In addition, users should be given agency to act upon the information they receive - If users can access personal data but are not able to change the way it is used by platforms there will be little accountability.

7. In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

17. Regulation of the design processes and business models of technology organisations, as well as their impacts, needs to strengthened. This places an onus on organisations to consider the impacts of their services during their design and take reasonable steps to mitigate them. A regulator can play an active role in this by encouraging transparency and understandability of technical processes, auditing them where necessary and intervening where design proposals don't meet a suitable standard. More broadly regulation can influence aspects such as professional standards that also have a significant impact on the design of technology.

18. Doteveryone's responsible technology programme[705] has also explored ways to make consumer technology products more responsible and accountable to society. This work has identified three core concepts that are central to the design of responsible technology:

    - Context - looking beyond the individual user and taking into account the technology's potential impact and consequences on society
    - Contribution - sharing how value is created in a transparent and understandable way

[701] http://attitudes.doteveryone.org.uk/
[702] ibid
[703] https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print
[704] http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Cranor_Formatted_Final.pdf
[705] https://doteveryone.org.uk/responsible-technology/

- Continuity - creating and supporting products and services that are safe, secure and reliable in a real-world environment, and ensuring people with different needs are accounted for in technology design.

19. These principles can be applied to a regulatory context in a number of ways. To ensure digital technologies are inclusive, standards for dark design patterns could be developed using a similar approach to the W3C Web Accessibility Initiative[706], and compliance with these standards could be made mandatory. For-profit platforms and services could be encouraged to be more transparent around their products' value flows or use of dynamic pricing, for example by reporting the value and source of revenues they receive from targeted digital advertising for each user. To consider context, technology organisations could be supported to carry out and report social impact assessments before their products reach market.

20. As Point 15 shows, platforms should also design legibility and understandability into their services. No user could face the cognitive load of understanding every process that happens when they open an app or make a transaction, but rather than designing for smooth, frictionless experiences, platforms should design for both understandability and explainability in both online and Internet of Things products. Frameworks such as the International Financial Reporting Standards (IFRS) provide a framework for understandability in the finance industry[707], and a similar common industry-wide standard should be developed and regulated for in the technology sector.

8. What is the impact of the dominance of a small number of online platforms in certain online markets?

21. The current regulatory approach of the Competition and Market Authority and other regulators is struggling to keep up with the evolving digital economy. The dominance of an small number of platforms, and more broadly technology companies such as Apple and Microsoft, is both symptom and a cause of this rapidly changing market structure. Four trends define this new system:

22. **The increasing influence of network effects.** Many tech companies are loss-making until they reach a critical mass of users. After this point network effects (where the value of a service to a user increases as more users join) often mean a platform can quickly become dominant in a short period of time[708]. Focusing on profitability as the primary indicator of market power can often mean that a regulator only intervenes after companies gain market dominance, at which point effective regulation becomes harder[709].

[706] https://www.w3.org/standards/webdesign/accessibility

[707] https://www.ifrs.org/issued-standards/list-of-standards/conceptual-framework/

[708] Ibid

[709] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1578762

23. **The changing role of 'price'.** Digital technologies have disrupted the traditional concept of price. Many platforms offer free-to-use services in exchange for users' data, making the notion of consumer price as an indicator of the health of a market redundant. latforms selling products and service may also deploy variable pricing and it can be hard to gauge where this practice is fair and where it's discriminatory. And on marketplace platforms, the price paid by a seller may differ from the amount received by a buyer and competition regulators also need to consider if all sides of this dynamic are treated fairly.

24. **Blurring of traditional market boundaries.** Some technology companies operate across multiple markets that have historically have had limited influence on each other (eg Amazon purchasing Whole Foods Market). With many services and sectors yet to be fully digitalised, there are concerns that large tech companies will gain an unfair advantage in emerging online markets[710]. Some companies may also cross subsidise services, where a service or product is sold at a loss to generate data that is valuable to them in other markets, as is the case with the Amazon Echo device[711]. The effects of combining data across different markets, and their influence on competition and consumer welfare, are not yet clear.

25. **Digital mergers and acquisitions.** It's common for large digital companies to acquire smaller, innovative start-ups[712]. Historically regulators considered the combined market power of mergers but it is now tricky to determine where digital organisations are acquiring potential future rivals, and whether that amounts to weakening competition.

26. Focusing on the impacts of the currently dominant platforms does not account for these underlying market changes, and regulators should instead look to modernise their approach so that they can address these root causes.

27. With many platforms and services adopting free-to-use data-driven business models and the rise of dynamic pricing, the use of product price as a key indicator for the health of a market is becoming increasingly redundant. Taking a more holistic view of consumer welfare, considering issues such as consumer privacy, value of personal data and the ability of consumers to switch between services, can give regulators a better understanding of how consumers' interests are affected by digital technologies.

[710] https://www.reuters.com/article/us-whole-foods-m-a-amazon-com-antitrust/critics-say-whole-foods-deal-would-give-amazon-an-unfair-advantage-idUSKBN19D2Q8

[711] http://speri.dept.shef.ac.uk/wp-content/uploads/2017/11/SPERI-IPPR-Digital-platforms-and-competition-policy-literature-review.pdf

[712] Giron Lopez, Jose Ali, Pierre Vialle, 'A preliminary analysis of mergers and acquisitions by Microsoft from 1992 to 2016: A resource and competence perspective', presented at 28th European Regional Conference of the International Telecommunications Society (ITS): Competition and Regulation in the Information Age, Passau, Germany, 30 July – 02 August 2017.

28. A more progressive approach to consumer welfare can also help to break down silos between regulators and promote a more collaborative approach. Taking the Facebook/Whatsapp merger as an example, data protection bodies expressed public concerns about data sharing following to the merger[713] - If competition regulators factored in privacy standards into their initial assessment US regulators may not have approved this deal[714].

9. What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

29. The importance of regulatory collaboration on an international level is also a recurrent theme in our current research on regulation. Many organisations Doteveryone spoke to during our own consultation felt the UK's attempts to regulate multinational technology companies in the absence of international collaboration would be toothless. Despite this some voiced concerns about existing global regulatory networks such as the Internet Governance Forum, which they criticised for excluding lower-GDP states and over-representing the interests of US-based organisations.

30. Against this backdrop many felt EU-level collaborations would be most effective for a UK regulator. With the UK currently likely to leave existing initiatives such as the EU Digital Single Market[715] and the EU Competition Network[716] after Brexit, developing a strategy for leveraging international networks will be an important part of fostering genuine accountability in multinational digital organisations.

10 May 2018

[713] See letter by the Chair of the Article 29 Working Party on the updated Terms of Service and Privacy Policy of WhatsApp in August 2016, https://www.cnil.fr/sites/default/files/atoms/files/20161027_letter_of_the_chair_of_the_art_29_wp_whatsa pp.pdf <

[714] https://globalcompetitionreview.com/article/usa/1147829/mcsweeny-privacy-competition-standard-could-have-sunk-facebook-whatsapp

[715] https://www.gov.uk/government/speeches/pm-speech-on-our-future-economic-partnership-with-the-european-union

[716] https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/67/67.pdf

Doteveryone, Julian Coles and Internet Society – oral evidence (QQ 28-34)

Transcript to be found under Julian Coles

Doteveryone – supplementary written evidence (IRN0103)

As part of oral evidence given on 8 May 2018

Question 7

a. *Do the characteristics inherent in internet and digital technologies require further powers for competition regulators, or is the current law effective in regulating the activities of platforms?*

1. Research comparing regulators and ombudsman across Europe highlights the effective role of collective redress, where groups of individuals affected by similar issues can take collective action against the same defendant.

2. Regulatory authorities which allow collective action are faster and more successful in addressing systematic infringements of market rules[717]. In the UK several regulators have shown the effectiveness of such powers, such as Ofwat returning £7 million to customers affected by Thames Water's misreporting of sewer flooding data.

3. Despite support from the ICO and civil society organisations[718] an amendment to the Data Protection Bill to allow for collective redress in situations where multiple individuals have been affected by a breach of data rights was not accepted by parliament.

4. Adapting the regulatory and legal system to strengthen mechanisms for collective redress for online digital issues is an important aspect of improving accountability from technology developers and users and promoting fair business practices.

b. *Is there a risk that the concentration of market power in the hands of a few companies might lead to social or cultural harms, including digital divides? Should a non-economic element be added to the market dominance test such as we media or content plurality?*

5. There is a need for a more holistic view of consumer welfare, considering not just price but also issues such as consumer privacy, value of personal data and the ability of consumers to switch between services.

6. This could help break down silos between regulators and promote a more collaborative approach. In the case of the Facebook/Whatsapp merger for example, data protection bodies expressed public concerns about data sharing following to the merger - If competition regulators

[717] http://www.fljs.org/sites/www.fljs.org/files/publications/Delivering%20Collective%20Redress%20in%20Markets-New%20Technologies.pdf

[718] http://tech.newstatesman.com/policy/data-breach-compensation

had factored in privacy standards, US regulators may not have approved this deal[719].

7. Some technology companies operate across multiple markets that have historically have had limited influence on each other (eg Amazon purchasing Whole Foods Market). The combination of data between these previously disconnected markets, in particular to build up increasingly detailed and nuanced marketing segmentation, means that market dominance tests must have a broader scope than individual sectors.

8. Collaboration between sectoral regulators must be encouraged and the skills to assess the competition impacts of combining cross-sectoral datasets and technologies must be strengthened by all regulators.

30 May 2018

[719] https://globalcompetitionreview.com/article/usa/1147829/mcsweeny-privacy-competition-standard-could-have-sunk-facebook-whatsapp

The Entrepreneurs Network & Adam Smith Institute – written evidence (IRN0070)

1 Introduction

1.1 This is a joint submission on behalf of The Entrepreneurs Network and the Adam Smith Institute. The submission was written jointly by Philip Salter (Founder, The Entrepreneurs Network) and Sam Dumitriu (Head of Research, Adam Smith Institute). We are grateful to the Lords' Communications Committee for providing us with the opportunity to submit evidence on the potential effects of internet regulation on startups, consumers, and the UK's tech sector (estimated to be worth £170bn to the UK's economy[720]).

1.2 The Entrepreneurs Network (TEN) is a think tank for the ambitious owners of Britain's fastest growing businesses and aspirational entrepreneurs. Through research, events and the media, it bridges the gap between entrepreneurs and policymakers to help make Britain the best place in the world to start and grow a business.

1.3 It supports the ambitions of our fast-growing network of 10,000+ members, through practical projects like The Leap 100 and Female Founders Forum.

1.4 The Entrepreneurs Network is also the Secretariat of the All Party Parliamentary Group (APPG) for Entrepreneurship, which sits across the House of Commons and House of Lords.

1.5 The Adam Smith Institute is one of the world's leading think tanks, ranked 2nd in the world among Domestic Policy Economic Think Tanks and 2nd in the world among Independent Think Tanks by the University of Pennsylvania. Independent, non-profit and non-partisan, we work to promote free market, neoliberal ideas through research, publishing, media outreach, and education. The Institute is today at the forefront of making the case for free markets and a free society in the United Kingdom.

1.6 Our Submission will focus on three key areas: the importance of preserving existing liability protections for online platforms and its effects on competition and innovation (addressing questions: 1, 2, 3, 8, and 9); the effect of data protection regulation on competition and innovation (addressing questions: 6 and 7); and the impact of large online platforms on consumer welfare, entrepreneurship and innovation (addressing questions: 2 and 8).

1.7 The submission will be structured as follows:

[720] *Tech Nation 2017*, Tech Nation, Accessed at: https://technation.techcityuk.com/

1.8 Existing liability protections for online platforms support innovation and promote competition.

1.9 Treating online platforms as publishers may lead to excessively risk-averse moderation or the rise of completely unmoderated spaces – neither is desirable.

1.10 Excessive data regulations can impose substantial costs on SMEs without providing significant benefits to consumers.

1.11 Competition between large online platforms is intense, but additional regulation may protect incumbents from insurgent startups.

1.12 Platforms may stimulate entrepreneurial activity within the UK by providing Corporate Venture Capital and opportunities for exit.

2 Existing liability protections for online platforms support innovation and promote competition.

2.1 Under the EU's eCommerce Directive internet intermediaries are exempt from secondary liability resulting from the illegal activity of its users, instead they are only responsible for taking down illegal content upon notification. By way of analogy, online platforms are treated as libraries rather than publishers. While a publisher of a libellous book may be liable, a library that innocently disseminates the book is not.

2.2 The EU's eCommerce Directive is Europe's version of the US' Section 230, described by Derek Khanna (Visiting Fellow of Yale Law School's Information Society Project) as the law "that cleared the way for the modern Internet", which created a good Samaritan exemption that enabled platforms to moderate content without being treated as a speaker or publisher.

2.3 Proposals to undermine eCommerce Directive liability protections include Lord Bew's suggestion that platforms should be liable for death threats and abuse directed towards politicians and recent appeals to replicate the recently passed controversial FOSTA-SESTA, which made platforms liable for facilitating prostitution (The Times, Mar 2018).

2.4 In 2017, Germany passed Netzwerkdurchsetzungsgesetz (NetzDG), better known as the Facebook Law, which required large platforms to take down 'obviously illegal' content within 24 hours of notification or face fines up to €50m. This is compatible with the EU's eCommerce Directive but raises similar issues to the prior laws.

2.5 Online services typically hire large numbers of workers to moderate their platforms. An estimate from 2014 suggests that over 100,000 people worldwide are employed as content moderators (Wired, Oct 2014). Facebook has 7,500 moderators alone (The Atlantic, Feb 2018), more than Snapchat and Twitter's combined total employee headcount. YouTube has pledged to deploy 10,000 staff to take down violent extremist content and content that endangers children (Telegraph, Dec 2017).

2.6 Google has developed technologies to proactively block illegal content. Content ID allows rights holders to tag content and then immediately blocks uploads of copyrighted content. However, not all tasks are equally automatable. Speech tends to rely on unspoken context that may be extremely difficult for algorithms to pick up on. For instance, an AI may incorrectly mark a sarcastic comment as a threat.

2.7 Imposing liability for user-generated content on online platforms poses significant risks to competition. The shift from human moderation, where costs scale with the size of the platform, to algorithmic moderation, where costs are fixed and there are large economies of scale, will advantage large incumbent platforms over insurgent startups. This may make investing in startup platforms less attractive and exacerbate funding gaps.

2.8 Without the certainty of Section 230 and the EU's eCommerce Directive, it's hard to imagine open platforms for online speech such as Facebook, Twitter, and Reddit developing. On Reddit, Derek Khanna (Wired, Sep 2013) writes:

2.9 "Let's assume the company's founders arranged a meeting with their Congressman and asked them to change the law to facilitate their market model for a message board on the Internet. What would most Congressmen think? Assuming they didn't get stuck with the Senator who referred to the Internet as "a series of tubes," it is likely that their elected representative would respond, "This is such a small market, and a silly idea, so why would we bother changing the law for you?" And yet, today Reddit is a billion dollar company and according, to one study, 6% of adults on the internet are Reddit users (myself, included)." (Khanna, Sep 2013)

3 Treating online platforms as publishers may lead to excessively risk-averse moderation or the rise of completely unmoderated spaces, neither is desirable.

3.1 Under publisher (rather than library) treatment, online platforms face substantial risks including large fines, civil lawsuits and other criminal sanctions. As a result, it may lead to risk-averse firms to over-police content, potentially chilling controversial but legal speech.

3.2 **Case Study A**: Under Germany's NetzDG, firms are not liable for illegal content but must take down 'obviously illegal' content (such as hate speech or pro-Nazi propaganda) within 24 hours of notification and other illegal content within 7 days. The law has faced criticism for incentivising Facebook and Twitter to remove legal political speech. For instance, the German satirical magazine Titanic had their twitter account suspended after parodying the anti-muslim comments of an Alternative für Deutschland (AfD) politician. Germany's biggest newspaper Bild called for the law to be abolished immediately and claimed the law was turning far-right politicians into "opinion martyrs" (Guardian, Jan 2018). The law has also been criticised by the Association of German Journalists (Reuters, Mar 2018).

3.3 **Case Study B**: In the US, since SESTA-FOSTA was passed, online platforms such as Reddit and Craigslist responded by closing discussion boards and removing all personals ads (Wired, March 2018). There are fears among vulnerable sex workers that the law will impede their ability to share 'bad client' lists on online platforms and will lead to riskier encounters (Broadly, Apr 2018). VerifyHim, the biggest dating blacklist on earth, recently announced that it was "working to change the direction of the site" (Wired, Mar 2018). According to tech advocacy group Engine: "Tech companies (large and small) regularly partner with law enforcement, the National Center for Missing and Exploited Children, and other anti-trafficking organisations." (Engine, Oct 2017) Dr Kimberly Mehlman-Orozco, a US human-trafficking expert witness who has served on many civil and criminal cases, believes that SESTA-FOSTA will make it harder for law enforcement to monitor sex trafficking cases, as advertisements shift from cooperative US-based open access websites to un-cooperative overseas based websites (Mehlman-Orozco, Jan 2018).

3.4 In an ideal system, platforms are empowered to pro-actively moderate distasteful or illegal content, while allowing for the free exchange of ideas. Shifting liability to platforms or creating strict penalties for inadequate compliance may lead to over-eager regulation and the censorship of useful services or legal speech. But if the category of publisher is interpreted excessively broadly (for instance, websites that engage in low-level curation or moderation) then there is a risk that websites may under-police content in order to maintain existing 'mere conduit' treatment. There are also risks that harmful content will shift to overseas un-cooperative websites.

4 Excessive data regulations can impose substantial costs on SMEs without providing significant benefits to consumers

4.1 It is important to assess the burden of data protection legislation upon SMEs (including startups and scale-ups). Poorly drafted or gold-plated legislation can advantage large incumbent businesses at the expense of smaller firms.

4.2 For instance, since May 2012 websites are required to notify users that they use cookies. The pop-up warnings, which are now seen on most websites, can be intrusive and impose time costs upon users. The compliance costs were substantial as firms were forced to re-design their websites to include cookie notices. According to the Information Technology and Innovation Foundation estimated that the directive cost UK firms as much as €600m based on a projected compliance cost of €900 per website (Castro and McQuinn, Nov 2014). Few consumers reported concerns about Cookies to the Information Commissioners Office (ICO). According to the ICO's own methodology, it "received just 38 'concerns' about cookies through the reporting tool on its website between

April and June 2014. By comparison, it had 47,465 complaints about unwanted marketing communications, which puts the cookie issue into perspective" (Econsultancy, August 2014).

4.3 The EU's General Data Protection Regulation (GDPR) is imposing similar high costs upon SMEs. As part of the regulation companies are required to gain explicit consent from users to gather personal information and send targeted marketing communications. According to W8 Data, only 25% of existing customer data meets the requirements specified under the GDPR (Campaign, Aug 2017). As a result, firms without requisite consent audit trails are sending out mass re-permissioning emails. However, response rates vary, and firms may lose significant amounts of marketing data.

4.4 There is evidence to suggest that the loss of marketing data under GDPR will lead SMEs to increase their reliance on Facebook and Google's advertising platforms. Google, for instance, "told website owners and app publishers that they would be required to gain consent for targeted ads on behalf of each of their digital ad vendors or risk being cut off from Google's ad network" (Wall Street Journal, May 2018). Facebook and Google have direct relationships with consumers, which makes it easier to gain explicit consent. This is not the case for smaller AdTech vendors that have B2B relationships with publishers, such as newspapers. Publishers are required to gain the consent of users on behalf of AdTech vendors that the user will never have heard of.

4.5 The law change is leading advertisers to shift marketing spend from smaller providers and towards Google and Facebook. Joachim Schneidmadl, chief operating officer for Virtual Minds AG, which owns German AdTech firms, was quoted in the Wall Street Journal saying "They are moving their money where there is clear, obvious consent. The huge platforms are really profiting." (Wall Street Journal, May 2018)

4.6 Regulation typically imposes greater relative costs upon smaller firms compared with large firms. As Facebook CEO Mark Zuckerberg stated at a Congressional hearing: "A lot of times regulation by definition puts in place rules that a company that is larger, that has resources like ours, can easily comply with but that might be more difficult for a smaller startup."

4.7 Research from London Business School's Professor Anja Lambrecht found that EU e-privacy regulations reduced venture capital inflows to Europe relative to the US. (Lambrecht 2017) She states, "our results are consistent with a view that tighter privacy policies may negatively affect VC investments into firms in online advertising, online news, and cloud computing."

4.8 Some AdTech firms are responding to the GDPR by leaving the European Union altogether. According to the Wall Street Journal, Drawbridge, which helps marketers track users as they switch from one device to another, abandoned its ad business in Europe as a result of GDPR, shutting its London office, said a spokesman for the California-based company (Wall

Street Journal, May 2018.)

4.9 Post-Brexit, there will be trade-offs however between regulatory divergence and the ability to move data from between the UK and the EU. In the Financial Times, European Leader Writer Alan Beattie argues that, "well-meaning motives about fixing a serious problem of genuine public concern are being distorted by cynical policymaking and thus facilitating covert protectionism in the form of rules requiring data to be held locally". (Beattie, Dec 2018)

4.10 If the UK leaves the Single Market and loosens the GDPR's requirements, British businesses may lose the ability to move data between the UK and EU. If this is the case then the benefits of reducing regulatory burdens will likely be outweighed by reduced access to European markets.

5 Competition between large online platforms is intense, but additional regulation may protect incumbents from insurgent startups

5.1 Large online platforms may possess large market shares in a single narrowly defined market, for instance Google's handles 75% of global search requests but competes intensely in other markets such as the more lucrative product search markets (where Amazon has greater market share).

5.2 The textbook economics model of perfect competition (many buyers, many sellers, homogenous products) is not directly applicable to many cases of real world competition. University of Liege's Professor Nicolas Petit argues "the antitrust monopolists may be firms engaged in a process of fierce holistic competition." (Petit, 2016)

5.3 Instead they compete through innovation and finding new and low-end footholds in markets. Petit again: "The disruptor targets the fringe of a market – customers not served or with low profitability – and progressively moves upmarket to erode the profitability of the incumbent." (Petit, 2016)

5.4 Tech companies guard against creative destruction by investing heavily in research and development. For instance, in 2014 Facebook spent $2.1bn on research and development representing 21% of its total revenue. By way of comparison, in the same year research-intensive pharma companies such as Roche, Novartis, or Pfizer did not spend more than 19% of total revenue on R&D. (Petit, 2016)

5.5 It has become conventional wisdom to argue that Big Data and 'Network Effects' have created winner-take-all markets that transformed Facebook and Google into natural monopolies. In an article for the journal *Regulation*, Prof David S. Evans and Prof Richard Schmalensee claim that the case has been overstated. (Evans and Schmalensee, 2018)

5.6 Evans and Schmalensee argue that the ability for consumers to use multiple social networking services all at once (multi-homing) (e.g. Facebook, Snapchat, Instagram, Twitter, Tumblr, and Slack) exposes large online platforms to competition. It is worth remembering MySpace was previously seen as an unassailable monopoly before Facebook eventually won out (Guardian, 2007).

5.7 For instance, WhatsApp was able to amass 400 million active users before being acquired by Facebook despite Facebook Messenger possessing a significantly larger userbase.

5.8 However, regulation can entrench incumbents and protect monopolists. The relative cost of regulatory compliance falls as a firm becomes larger. Assigning liability to online platforms or imposing stricter data regulation may increase the risk associated with investing in tech firms at an early stage and restrict consumer choice.

6 Platforms may stimulate entrepreneurial activity within the UK by providing corporate venture capital and opportunities for exit.

6.1 Data garnered from social media, helps entrepreneurs better understand their customers and increases their likelihood of making sales and pivoting their product or service towards the needs of customers.

6.2 Platforms have increased the number of ways businesses can market their activities to customers. This has increased competition, saved time and reduced costs.

6.3 The ability to target niche customers at a low cost means startups are better able to compete with larger companies.

6.4 One factor for anyone deciding to start a business is when they will exit to realise the value of their risk and hard work. As Petit explains: "IPO is indeed a rather exceptional exit route for startups. Instead, many technology startups ambition is exit through M&A with a larger firm. This is the path followed by Android, Skype, Huffington Post, WhatsApp, Instagram, Oculus, Minecraft, Beats, Twitch, Waze, LinkedIn and others." (Petit, 2016)

6.5 This is a particularly important consideration for the founders of fast-growth firms, which are more likely to be more productive – anything that hinders the flow of M&A activity would have an impact on high-value entrepreneurial activity.

6.6 **Case Study C**: Facebook has acquired the following UK companies: Lightbox.com, a photo sharing company (May 2012); Monoidics, an automatic verification software company (July 2013); Ascenta, a high altitude unmanned aerial vehicle company (March 2018); Surreal Vision, an augmented reality company (May 2015); Two Big Ears, a spatial audio company (May 2016).

6.7 **Case Study D**: Alphabet (formally Google) has acquired the following UK companies: PlinkArt, the virtual search engine (April 2010); Phonetic Arts, the speech synthesis company (December 2010); BeatThatQuote.com, the price comparison service (March 2011); DeepMind Technologies, the artificial intelligence (AI) company (January 2014); spider.io, the anti-click fraud company (February 2014); Rangespan, the e-commerce company (May 2014); Dark Blue Labs & Vision Factory, an AI company (October 2014).

6.8 Platforms have venture capital arms, investing significant capital into the UK. For example, Alphabet's GV (formally Google Ventures) recently invested $14.5m into the UK-based augmented reality (AR) firm Blue Vision. Last year, GV took part in $25m investment round of Currencycloud, a UK payments startup.

Bibliography

Beattie, A. (Dec 2018) "EU trade data flows are becoming the new GMOs" *Financial Times*

Castro, D. and McQuinn, A. (2014) "The Economic Costs of the European Union's Cookie Notification Policy", *The Information Technology and Innovation Foundation*.

Charlton, G. (Aug 2014) "The EU 'cookie law': what has it done for us?", *Econsultancy*

Chen, A. (Oct 2014) "The Laborers Who Keep Dick Pics and Beheadings Out of Your Facebook Feed", *Wired*

Evans, D. and Schmalensee, R. (Jan 2018) "Debunking the 'network effects' bogeyman" *Regulation*

Harper, T., Shipman, T., O'Connor, M. and Fortson, D (Mar 2018) "Google and Facebook among giants "making profit' from pop-up brothels" *The Sunday Times*

Keegan, V. (Feb 2007) "Will Myspace ever lose its monopoly", *The Guardian*

Khanna, D. (Sep 2013) "The Law that Gave Us the Modern Internet—and the Campaign to Kill It", *The Atlantic*

Lambrecht, A. (2017) "E-Privacy Provisions and Venture Capital Investments in the EU" *Centre for European Policy Studies*

Madrigal, A. (Feb 2018) "Inside Facebook's Fast-Growing Content-Moderation Effort", *The Atlantic*

Mehlman-Orozco, K. (Jan 2018) "Legislation aiming to stop sex trafficking would hurt investigations" *Homeland Security Today*

Mendick, R. (Dec 2017) "YouTube boss pledges to step up war on violent extremism with 10,000-strong internet police force", *The Daily Telegraph*

Oltermann, P. (Jan 2018) "Tough new German law puts tech firms and free speech in spotlight", *The Guardian*

Petit, N. (2016) "Technology Giants, the Moligopoly Hypothezis and Holistic Competition: A Primer."

Schechner, S. and Kostov, N. (May 2018) "Google and Facebook likely to benefit from Europe's privacy crackdown" *The Wall Street Journal*

Stryker, K. (Apr 2018) "6 sex workers explain how sharing client lists saves lives", *Broadly*

Tan, E. (Aug 2017) “GDPR will render 75% of UK marketing data obsolete”, *Campaign*
The Engine Team (Oct 2017) “Testifying on Section 230” *Engine*

Thomasson, E. (Mar 2018) “Germany looks to revise social media law as Europe watches”, *Reuters*

Tiku, N. (Mar 2018) “Craigslist shuts personal ads for fear of new internet law”, *Wired*

May 2018

Dr David Erdos[721] – written evidence (IRN0074)

Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

1. Whilst it would seem at best premature to seek over-arching regulation of the internet, it would be a mistake to consider that the law envisages the internet as an unregulated space. Not only to laws and regulations crafted for an offline era apply, in principle, also online but a number of laws have already been adopted which seek to respond to new digital realities. Most notably, the entire law of data protection is primarily orientated towards the regulation of the processing of personal information using electronic means. Meanwhile, the e-Commerce Directive 2000/31/EC was also designed to begin the process of establishing a coherent regime for information society services online.

2. A great range of regulatory regimes, therefore, have application to the internet and some of these have been specifically crafted with an eye to it. Moreover, as the internet has grown more powerful (to do harm as well as of course much good), so a greater range of public bodies have or should have become engaged in this space. This includes not only the Information Commissioner's Office and Ofcom but also the Children's Commissioner, Competition and Markets Authority, Equality and Human Rights Commission and the Intellectual Property Office.

3. Many of these regulations and regulators confront many similar challenges, notably, how to craft a regime which secures effective redress for harms which occur online. There is therefore a great need for more 'joined-up' regulatory thinking and work here. At a pan-European level, the European Data Protection Supervisor's facilitation of a Digital Clearinghouse[722] may provide something of a model here, albeit one which is only in the very early stages of gestation and lacks any clear budget. It seems that something similar (but more formalized and better resourced) would be valuable to establish at national level also. The could be the prelude for even more cooperation in the future.

What should the legal liability of online platforms be for the content that they host?

4. There is a danger of answering a question such this in overly binary form. 'Online platforms' cover a myriad of different services and exercise very different levels of control over their operation. Indeed, at a technical level, 'hosting' is only one of many processing operations that the more active platforms perform. Indeed, following on from the logic of C-131/12 *Google Spain* (see especially [35]-[37]), it should be recognised that it is often the pulling, pushing and aggregation of content which fuels the harms

[721] Deputy Director, Centre for IP and Information Law; University Senior Lecturer in Law & the Open Society; WYNG Fellow in Law, Trinity Hall, University of Cambridge

[722] See https://edps.europa.eu/press-publications/press-news/blog/digital-clearinghouse-gets-work_en.

experienced online. Moreover, such further processing (and its related monetization) is very often substantially under the (albeit algorithmic) control of platforms themselves.

5. The activity of online platforms very often does engage freedom of expression and requires a balance between competing rights or weighty public interests. Notwithstanding, the liability and responsibility of online platforms should increase as they exercise greater autonomous control over processing. Thus, whilst those who are genuinely solely operating under the authority of users should only be subject to a specific 'notice-and-takedown' regime, applicable in cases where it is impracticable to pursue the user themselves. On the other hand, those who exercise more autonomous control processing should be expected to assume greater duties of care[723] including (in so far as applicable):

   - Having clear and prominent policies concerning acceptable content,
   - Responding proactively to systematic violations of such policies,
   - After being put on constructive notice, taking reasonable steps to fully investigate potential illegality and undertaking a *bona fide* and careful assessment of this,
   - Adopting, where practicable and proportionate, continuing measures (including in some cases filtering) to prevent the repetition of specific illegalities.
   - Ensuring that their own additional processing (e.g. adoption of facial recognition) does not itself violate applicable legal standards.

6. The practical filling out of these responsibilities should take into account the serious of the risk of interference with rights and weighty interests on each side of the equation. In this context, the divergent resource capacity of otherwise similarly situated internet platforms should be taken into account. Nevertheless, in a society which takes the vindication of the law of rule seriously including online, the failure of an 'active' platform to discharge the minimum standards outlined above should be recognised as incompatible with that service's duty of care as an at least semi-autonomous operator.[724] Finally, the capacity of at least the larger online operators to act in innovative and sometimes resource-intensive ways should not be underestimated. Alphabet (the parent company of Google)

[723] It is possible that such additional duties could, in principle, be limited to activities which engage the autonomous or semi-autonomous activity of these platforms (e.g. pushing, pulling, aggregation etc.). However, in reality, such processing is so fused to the passive hosting that this may make only a limited difference in practice.

[724] For a detailed elaboration of this approach, albeit only within the specific area of data protection, see the following Working Paper: David Erdos, 'Delimiting the Ambit of Responsibility of Intermediary Publishers for Third Party Rights in European Data Protection: Towards a Synthetic Interpretation of the EU acquis in the Era of Regulation 2016/679" (2017) (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993154). The final version of this paper will be forthcoming shortly in the *International Journal of Law and Information Technology*.

reported an annual turnover in 2017 in excess of $100bn,[725] an amount which is greater than the entire GDP of a number of medium-sized countries. Meanwhile, Facebook's turnover was in excess of $40bn,[726] which is also very considerable.

7. This general approach should be seen as building on, rather than inconsistent with, the e-Commerce Directive 2000/31/EC. To begin with, this Directive was originally conceived as only partially governing liabilities and responsibilities within this space. Most notably (and problematically) the Directive did not seek to govern the responsibilities and liabilities of search engines and other "location tool services" as regards the content which they indexed. Instead, it only included a re-examination procedure which has never been properly carried forward.[727] As originally drafted, the Directive was also not even intended to cover the very active hosts that are now ubiquitous.[728] Even within its area of application, the Directive is open to the variegated approach to regulation as outlined here. Most notably, recital 48 states that the Directive "*does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activity*". Meanwhile, article 15(2) specifically provides that Member States may oblige service providers benefiting from intermediary shields promptly to inform competent public authorities of alleged illegal activities and (at their request) also communicate information "*enabling the identification of recipients of their service with whom they have storage agreements*".

8. This variegated approach is also being increasingly recognised in legal interpretation and initiatives. For example, the implications of what it means for operators such as search engines[729] and social networking sites[730] to be both intermediaries and also data protection controllers is an ongoing interpretative challenge. Meanwhile, the European Commission's Digital Single Market initiatives which attempt in the areas of 'hate speech' and child protection[731] as well as copyright[732] to set out measures[733] to

[725] http://money.cnn.com/2018/02/01/technology/google-earnings/index.html

[726] https://investor.fb.com/investor-news/press-release-details/2018/facebook-reports-fourth-quarter-and-full-year-2017-results/default.aspx

[727] Directive 2000/31/EC, art. 21(2).

[728] See Erdos, 2017, p. 8.

[729] See e.g. C-131-12 *Google Spain*.

[730] See e.g. *CG v Facebook, Joseph McCloskey* [2016] NICA 54.

[731] European Commission, *Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities* (COM (2016) 287 final).

[732] European Commission, *Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market* (COM (2016) 593 final).

[733] The proposal on hate speech and child protection, which extends only to "video-sharing platforms" (*supra* note 731, p. 29), specifies that such positive measures shall consist of the following as appropriate: (i) defining and applying terms and conditions in these two areas, (ii) establishing and operating mechanisms for users to report or flag problematic content, (iii) explaining to users what effect has been given to such reporting and flagging, (iv) enabling users to rate content, (v) establishing and operating age verification systems in relation to content and (vi) providing parental content systems with respect to age-related content (*supra* note 731, pp. 29-30). Meanwhile the copyright proposal, which encompasses "[i]nformation society service providers that store and provide to the public access to large amounts of works or other subject-matter uploaded by their users"

address some of the real harms associated with certain intermediary publication activities adopt a similar duty of care approach. Whilst all of these developments raise multiple detailed conundrums, the general direction of travel seems correct and indeed overdue.

How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

9. Platforms decision to tackle potential online harms can impact the rights and interests of other parties including any purported victims of harms (which are often, albeit generally only via algorithm, substantially facilitated by the platform themselves) and the original uploader of any material. Anecdotal evidence suggests that online platforms may not be investing enough resources in effectively and carefully moderating content and may often be focusing not on standards set down in law but rather on their own often much vaguer and discretionary terms of service.

10. Online platforms are private entities and, in principle, benefit from all the concomitant liberal freedoms which come with that status. Nevertheless, they do have various responsibilities to be transparent as regards their processes for managing content processed in their services.[734] However, some specific forms of transparency may come into serious conflict with a platform's duties to address, rather than exacerbate, the harms in question. This issue has been highlighted by internet search engines' practice to individually notify webmasters of particular cases of de-indexing under European data protection and without any safeguards. In some cases, this has resulted in individuals with a *bona fide* 'right to be forgotten' being subject to unpreceded new publicity. This practice has been found to be illegal by the pan-European Article 29 Working Party (shortly to become the European Data Protection Board)[735] and has even led to the Spanish Data Protection Authority fining Google for its notification practices.[736]

11. General transparency should only very rarely come into serious conflict with other rights and weighty interests and platforms should therefore work

(*supra* note 732, p. 29) would require such services to take "appropriate and proportionate" measures such as "the use effective content recognition technologies" to implement agreements concluded with rightsholders or to the prevent the availability of works or other subject matter identified by rightsholders which fall outside such agreements and, further, that the provide the latter "with adequate information on the functioning and development of the measures, as well as, where relevant, adequate report on the recognition and use of the works or other subject-matter" (*supra* note 732, 29-30).

[734] Notably, as regards natural person users, such transparency may flow from requirements now set out in the General Data Protection Regulation 2016/679.

[735] See European Union, Article 29 Working Party (2014), *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12* (2014) (http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf), p. 10.

[736] See Erdos, David, *Communicating Responsibilities: The Spanish DPA targets Google's Notification Practices when Delisting Personal Information* (2017) (https://inforrm.org/2017/03/21/communicating-responsibilities-the-spanish-dpa-targets-googles-notification-practices-when-delisting-personal-information-david-erdos/).

harder to ensure such transparency.[737] Specific transparency, however, can pose a risk to other rights and freedoms and in some circumstances these may be so serious as make this simply inappropriate or even illegal.[738] Where specific transparency does pose a significant and particularised risk to rights and/or weighty interests but could be considered outweighed by the rights of users, then platforms should investigate the possibility of engaging in safeguarded forms of disclosure as also suggested by the Article 29 Working Party. In other circumstances (e.g. the routine removal of copyright-infringing content) specific notification to users should not pose a significant particularized risk to rights and/or weighty interests and therefore should take place.[739]

12. Some form of transparency is a necessary prelude to holding online platforms to account including legally vis-à-vis the moderation of their services. Those reporting purposed illegalities rightly generally have the ability to go to the relevant competent authority including potentially the Information Commissioner's Office, Ofcom or even the police. At least in principle, they may also be able to seek redress directly in court.

13. The position of the aggrieved uploading user who feels that the platform has gone beyond what is legally required is more problematic. Given their private nature, it may in principle be questioned whether the State should seek to heavily regulate a platform's own approach to moderating terms which go beyond ensuring mere legal compliance. Such terms may legitimately reflect a platform's individual *ethos*. Nevertheless, platforms must be held legally accountable for fairly applying any terms and conditions which they do set down. Moreover, any analysis of this area cannot avoid the reality that the market for platforms is currently highly oligopolistic in nature, a reality which appears at least exacerbated by network effects which are endemic to today's internet. Given this, it may well be that highly discretionary or arbitrary terms could represent "unfair" terms within the meaning of the *Unfair Terms in Consumer Contracts Regulations* 1999. In principle, users should already have theoretical redress in this regard through the courts. However, in practice, this would be beyond the reach of all but the most dedicated and well-resourced individuals.

14. In addition to making terms as clear, reasonable and precise as possible, platforms can and should guard against unfairness by administering effective mechanisms to appeal decisions either themselves or through an arms-length industry body. Ultimately, it seems important that such terms and procedures are subject to supervisory regulation. This would best be

[737] *Ibid*, p. 10.

[738] For example, even Google accept that it is not appropriate to notify a "revenge porn" site of the de-indexing of its content.

[739] On the other hand, the publication and continued indexing of such content through cooperation with entities such as the Lumen Database results in a failure to truly remove such content at all, a result which is extremely problematic from the perspective of securing effective redress for all manner of online harms. For more regarding concern on this issue see Ernesto, *Court Orders Google to Remove Links to Takedown Notice* (2017) (https://torrentfreak.com/court-orders-google-to-remove-links-to-takedown-notice-170616/).

carried out by a consumer protection authority.[740] Unfortunately, the recent abolition of the Office of Fair Trading would appear to leave a serious gap in UK regulation in this regard.

What role should users play in establishing and maintaining online community standards for content and behaviour?

15. Users have an important but limited part to play in the policing of standards on online platforms.

16. Turning first to ensuring compliance with the law itself, they can and should play an important role in bringing to the attention of platforms "*facts or circumstances [or indeed more] on the basis on which a diligent economic operation*" should then identify illegality (C-324/09 *L'Oréal* at [120]). Indeed, not only has the Court of Justice stressed "*every situation*" (*Ibid* at [121]) where such awareness/knowledge comes to the attention of a service must be covered but article 5(1)(c) of the e-Commerce Directive 2000/31/EC explicitly requires that information society services render "*easily, directly and permanently accessible to the recipients of the service*" "*at least*" "*the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner"*. It is a matter of grave and legitimate concern that many online platforms restrict the matters which can be brought to their attention electronically (or some cases even via a geographic address), failing to provide any generic electronic address by means of which they can contacted as per Directive 2000/31/EC's article 5(1)(c).[741] Unfortunately, regulatory action to secure compliance with this also seems to be largely absent.

17. Ultimately an assessment of the legality (or otherwise) of information (or activity) online needs to be informed by careful, legally-qualified advice. This task cannot be outsourced to a shifting and amorphous group of users themselves.

18. As regards the policing of a platform's own terms (going beyond mere legal compliance), there may well be more potential for users themselves to both evolve and police relevant standards. However, such standards and their application in each individual situation should be as clear, reasonable and precise as possible. Platforms themselves must remain responsible for ensuring that such standards are met.

What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

19. Assuming that the UK does leave the European Union then it will have more opportunity to develop a distinctive approach to the regulation of internet harms. However, the extent of such additional discretion, would very much

[740] See European Union, *Common position of national authorities within the CPC Network concerning the protection of consumers on social networks* (n.d./2017) (http://ec.europa.eu/newsroom/document.cfm?doc_id=43713)

[741] Ibid.

depend on any final exit agreement. In any case, it seems likely that, as a continuing member of European family of liberal democratic nations, the UK would want to continue to develop its policies in general alignment with evolving pan-European approaches. In this regard, it should be noted EU membership in any case grants the UK considerable flexibility in specifying reasonable duties of care and adopting a more variegated approach to regulation. This is particularly the case given that pan-EU thinking is, in many areas, evolving on much the same lines as that of the UK (see, for example, the ‘hate speech’ and child protection as well as copyright proposals noted above).

20. Whilst an exit from the EU may grant the UK some welcome new flexibility, there is an acute risk that it could lead the UK exercising less influence over the practical evolution of internet policy and harm the, in any case very weak, regulatory frameworks which do operate here. The internet is a uniquely transnational environment and its effective regulation often requires transnational cooperation. Many of the practical initiatives to regulate this space (including, as noted elsewhere in this submission, in the area of hate speech, child protection, consumer protection and data protection) have at least been coordinated within an EU context and have often even been championed by it. Withdrawal of the UK from such initiatives may damage these efforts to effectively regulate the internet and result in a loss of a ‘UK voice’ as to how such efforts should evolve going forward.

11 May 2018

eSafe Global Ltd – written evidence (IRN0022)

Submission on behalf of eSafe Global Ltd (formerly eSafe Systems Ltd) by Mark Donkersley CEO

1. BACKGROUND

1.1. The Government's green paper issued by DCMS on 11 October 2017 envisages a code of practice for social media companies and communications service providers. This is to be funded by a voluntary levy with the objective of creating a regime to support awareness of, and create preventative activity to counter, internet harm.

1.2. "Safety by Design" is the philosophy proposed in the green paper with the bulk of the levy to be assigned to education programmes for users and applications producers. This is seen as a necessary condition to "ensure that Britain is the safest place in the world to be".

2. RESPONSE

2.1. In responding to Question 1 only of the select committee's brief i.e. "is there a need to introduce specific regulation for the internet?", it is eSafe Global’s contention, based on real time monitoring of 750K+ pupils and staff in the education system in England and Wales, that:

2.1.1. the necessary condition will not be achieved on a voluntary basis and any code of proposed practice will have to be enforced via legislation: much like the Data Protection bill with fines (on a percentage of corporate turnover) for breaches.

2.1.2. even if this necessary condition is achieved it will not be properly effective unless a sufficient condition is in place. That sufficient condition is "Safety by Inspection". This requires real time high quality monitoring of evidential harms such that INCIDENCE DATA is available for early intervention to mitigate damage, especially to the mental health of young people, and TREND DATA available to those charged with public policy formation for future legislative action in harm prevention.

2.2. Over the past two years we have made and presented these points to parliamentary select committees chaired by Lord Best, Sarah Wollaston and Alex Chalk. We would invite the present select committee to study the confidential incidence only statistics (based on a data sample of 150 secondary level schools during the autumn term 2017) in section 3 Statistics below to gain an understanding of the current range of harmful behaviours. We would be happy to supply the equivalent trend data on request.

2.3. This intelligence- led monitoring will not (for the foreseeable future at least) be actionable via technological/artificial intelligence solutions. Investment in front line people capable of the sensitive interpretation of a wide range of often nuanced behaviours will be required.

2.4. We would encourage the select committee to embody such thinking in any future regulatory design.

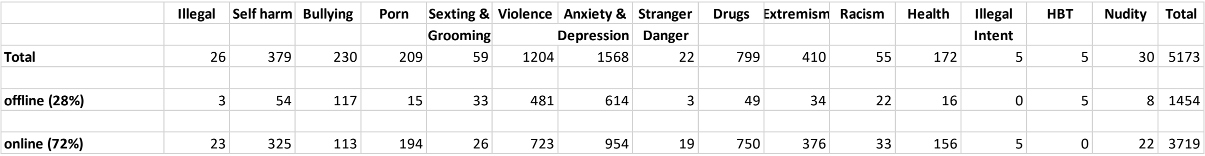
3. STATISTICS

3.1. The data sample of 138,841, 11-18 years old pupils across 150 secondary level schools and represents approximately 18% of the entire school population monitored by eSafe in England and Wales.

3.2. The sample data extracts are an indication of the granularity and extent of online and offline behaviour analysis, by incident category and application, across the digital environments used by young people in primary, secondary and further education in England and Wales.

3.3. Table 1 illustrates the extent of serious behaviour markers detected and escalated by eSafe across the school sample. The variance between online and offline behaviour in the digital environment is consistent with incident analysis from the last six years.

Table 1: Total number of serious category incidents escalated by eSafe during the autumn term 2017



	Illegal	Self harm	Bullying	Porn	Sexting &	Violence	Anxiety &	Stranger	Drugs	Extremism	Racism	Health	Illegal	HBT	Nudity	Total
					Grooming		Depression	Danger					Intent			
Total	26	379	230	209	59	1204	1568	22	799	410	55	172	5	5	30	5173
offline (28%)	3	54	117	15	33	481	614	3	49	34	22	16	0	5	8	1454
online (72%)	23	325	113	194	26	723	954	19	750	376	33	156	5	0	22	3719

3.4. Table 2 reveals the prevalence of serious incidents by online application. The 13 most common applications account for 85% of the serious category incidents in the digital environment provided by schools in this sample.

Table 2: Prevalence of serious category 'online' incidents during the autumn term 2017 by application (top 13 only)

Online	Illegal	Self harm	Bullying	Porn	Sexting	Violence	Anxiety &	Stranger	Drugs	Extremism	Racism	Health	Illegal	HBT	Nudity	Total
					Grooming		Depression	Danger					Intent			
Google	17	175	21	90	5	228	341		473	192	17	84	4	2	12	1661
URL bar	4	79	9	19	2	119	220		157	97	4	47	1			758
Bing.com		17	8	15		25	49		57	41	1	12			1	226
Youtube.com	1	15	3	9		33	45		22	23	1	1				153
unblockvideos.com				3												3
Google Translate		5	15			61	48		9	3						141
0123movies.com																0
Google Docs		6	17	1	4	44	33		3		3	1				112
Google Mail		1	9		1	27	22	2				2			1	65
putlockers.fm																0
tubeunblock.me							1									1
www.amazon.co.uk		1		1					3	1		1				7
Facebook		4	3		5	9	5	2	3							31

3.5. By way of comparison to Table 2 above, Table 3 reveals the prevalence of serious incidents by offline application. The 13 most common applications account for 86% of the serious category incidents in the digital environment provided by schools in this sample.

Table 3: Serious 'offline' incidents at secondary level by application during the autumn term 2017

Offline	Illegal	Self harm	Bullying	Porn	Sexting &	Violence	Anxiety &	Stranger	Drugs	Extremism	Racism	Health	Illegal	HBT	Nudity	Total
					Grooming		Depression	Danger					Intent			
Word Document		18	23		5	156	218		24	12	11	7				474
Outlook		5	61	2	15	124	60	3	6	4	6	2		1		289
PowerPoint	1	14	10		1	22	114		7	2		2		1		174
Python		2	5		1	37	52		2	4						103
Windows Desktop			1	1	11	8	18				1					40
Windows Search Tool		4	2			13	12				1	1		1		34
Sticky Note		5	4			9	11			1				1		31
Notepad			2			13	11				2					28
My Computer	1					6	9		5	1						22
Excel						9	15									24
Publisher Document						8	10		1	2						21
Windows Photo Viewer		3		3		1						2			8	17
DreamWeaver						2	7					1				10

11 May 2018

Facebook – written evidence (IRN0098)

Introduction

Thank you for offering us the opportunity to respond to your inquiry. We welcome the House of Lords Select Committee on Communication's contribution to this important debate.

At Facebook, we are proud to be significant investors in the UK economy and last year celebrated a decade in the UK. Since coming to the UK 10 years ago, we have grown our workforce to over 1,800 full time employees. We opened a new office in London in December and have plans to have increase our UK workforce to 2,300 employees by the end of year. The UK is our largest engineering hub outside of the US and we have developed some of our most significant products here. Over 300 million users worldwide are connected to a UK business on Facebook, and over 2 million UK businesses have a presence on Facebook.

We greatly value our work with policymakers to ensure that we harness the great benefits and opportunities provided by the internet, while acknowledging that we need to work together to mitigate the potential harms and challenges that may arise online. We are eager to work with policymakers such as your Committee to ensure that people have the tools, resources and support they need to stay safe online and that platforms meet their responsibilities to provide a safe environment.

With 40 million people using Facebook in the UK every month to connect with each another and share the things that matter to them, we recognise that we have an important role in the social, democratic and economic life of the UK.

Although in the main we have seen many different positive uses of our service, we're acutely aware that it can also be used to harm or attempt to harm. As stated in the Government's Internet Safety Strategy green paper, 99% of teenagers have seen people posting things online that are 'supportive, kind or positive'. By comparison, 20% of teenagers encountered something online that they 'found worrying or nasty in some way'.

The safety of our community is our top priority and we take significant steps to ensure that Facebook remains predominantly a force for connecting people, improving dialogue and building communities.

We have outlined our response to the questions put forward in your Committee's call for evidence and hope the facts and discussion points set out below will be useful.

UK Government Proposals

The UK Government has a number of ongoing processes to develop codes of practice or consulting on requirements for internet companies. We are fully engaged with those processes and in many areas support action, whether voluntary or legislative. It is important in considering measures such as these to remember that not all companies are the same. Facebook is one social media platform in a sector that includes many smaller businesses. The measures we outline below are not always possible for all platforms - even for some who may be very big in terms of users in the UK.

The Government's approach in the recent response to the Internet Safety Strategy consultation of seeking consensus, of building on existing good work and of seeking to raise standards across the board will serve as a useful framework for discussion as we move towards a White paper later this year.

Responsibilities and regulation

1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

At the outset, it is worth noting that there is extensive regulation that applies online and for internet companies. Under the e-Commerce Directive platforms have significant responsibilities to remove illegal content when notified. In addition the EU General Data Protection Regulation fundamentally regulates the way that platforms such as Facebook can handle data. There is a range of other broad regulatory frameworks, for example covering competition, which equally apply to the online and offline environments.

Facebook believes it has a broader sense of responsibility including in relation to the content on our platform and the experience of our users. At Facebook, we believe everyone online should be empowered to manage risks and stay safe and that technology companies have a responsibility to take action to protect people from harmful content.

Facebook has taken significant steps to regulate the platform and ensure that harmful content is either removed or prevented from reaching our platform. We are not waiting for legislators and regulators to devise new forms of regulation. We share the concerns of policymakers and are already working on many of the same issues. Examples of this in the areas of content moderation and online safety are set out below. Regulation relating to content, which is the most commonly suggested form of new regulation, should acknowledge that responsible platforms already see their interests as aligned with the goal of removing harmful content.

The Government makes the point that what is illegal offline should be illegal online. Facebook respects UK law and removes content where agencies report to us that it breaches the law in the UK, even if it does not violate our community standards. We publish the total numbers of these instances; such cases are relatively rare in the UK in part because our terms of service are similar to, or in many areas go beyond the standard of UK law.

Facebook is a place where people and organizations (including millions of businesses, charities and campaigning organizations) post and create their own content - whether that's a status update, or a comment on a friend or family member's photograph, a research paper or story. Our service enables millions of people to have a voice that they have never had before. We allow and encourage people to communicate with one another freely. This takes place in an environment where users are, quite rightly, not expecting their speech to be monitored and potentially edited before they post online. Changes to the legal framework would need to recognise this important aspect of online spaces.

Another important consideration is that it is greatly in our interests to self regulate the content on our platform - to ensure user and public confidence, and to ensure our platform is a space where the vast majority of users feels safe and where users wish to come and share their personal experiences and the things they care about.

That is why we work hard to enforce our community standards, as quickly and effectively as possible using technology, review teams and other resources. A new law designed to change those incentives would have to show that it did so in a way which improved the outcomes it sought to address. Some of the commonly suggested models have created significant perverse incentives - for example, rewarding platforms that make it hardest to report concerns, or causing platforms to over-block significant amounts of legitimate speech in order to avoid risk.

2. What should the legal liability of online platforms be for the content that they host?

The internet has flourished in part because intermediaries are not required to pre-review or monitor what people can say or share or do online, with limits to the degree to which platforms and internet service providers are legally liable for content created by users. Ministers and others have repeated their view that the internet services people rely on could not foster the innovation and economic opportunity they do today without this being the case. Changes which did not reflect this reality risk making it impossible for certain services to exist at all.

Facebook is already under an effective obligation to remove illegal content when it is notified of illegality - in fact, our liability protection depends on our acting when we receive actual knowledge about illegal content.

So we are explicitly talking about legal liability for content that platforms do not know about when we talk about removing liability protections.

Removing intermediary liability protections would invite abuse because intermediaries would have strong incentives to comply with all removal requests - whether it was a political party seeking to censor an inconvenient viewpoint or a restauranteur looking to suppress a review of a bad meal. The safest course would always be to remove content alleged to be illegal by any party, rather than risk paying fines or facing other sanctions.

Nevertheless, we understand why policy makers and commentators are exploring whether and how platforms like Facebook should be more regulated. We have long supported discussions about how the regulatory environment could work better to achieve our objective of ensuring everyone has positive experiences online.

We are open to working with Government to think through these challenges. Where legislation can raise standards across the board, or can create clarity where its absence makes taking action harder, we think there could be merit in Government action. This will often not touch directly on the issue of liability but might make clearer what content is considered legal or illegal.

For example, we think that transparency for political advertising online could be better regulated, as it is offline. We are making significant changes in this area - requiring transparency on our platform in time for the May 2019 local elections as set out below. But we also want to work with the Electoral Commission and the Government to establish clear rules in this area.

In other areas, such as harassment cases which are predominantly offline, or hate speech, clarity in the law would ensure that police, users, prosecutors and platforms could have greater confidence that the system is working. And quicker, clearer notices from courts would also ensure that platforms were better able to assess content that was reported to us, with better context.

Content moderation and online safety

3. How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content and behaviour? Who should be responsible for overseeing this?

4. What role should users play in establishing and maintaining online community standards for content and behaviour?

5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information

The safety of people who use Facebook is our most important responsibility. As part of our commitment to achieving this, the first step is to create strong and detailed policies. When people come to Facebook, we always want them to feel welcome and safe. That’s why we have rules against content and behaviour such as bullying, harassment, credible threats, graphic violence, the sexual exploitation of minors, and the non-consensual sharing of intimate images.

At Facebook we aim to provide people with the tools they need to manage their experience on our platform. This includes tools and features related to privacy, security, as well as tools related to conflict resolution, blocking and reporting. Every piece of content on our platform can be reported to us via the user-friendly reporting links which appear beside each piece of content. To ensure that enforcement of our policies is fair and transparent, we always 'close the loop' with the person who reported the content, to let them know what action we have taken (or otherwise) with regards to their report, or to provide them with additional resources - for example directing them to expert services.

In addition to the tools provided to allow people to report content, we also look to take proactive measures to identify harmful content and remove it from our platform. We are using and investing in a variety of automated techniques to help us more quickly identify and remove bad content, and particularly spot it before it is published online. These include photo and video matching; fanouts from disabled content; and machine learning on language from violating posts. So far, we have focused this work on the most harmful online activity - terrorist and child exploitation. We work closely with relevant law enforcement bodies and the Internet Watch Foundation in these areas. Technology will be a great help in tacking this problem. But there are significant limitations to how much it can currently achieve- and these limitations will continue. Human reporting and reviewing will remain a significant part of managing content online.

Facebook is strongly committed to an effective, fair and transparent approach to the moderation of content on the platform. This commitment is illustrated by the recent steps we have taken:

- For years, we've had public Community Standards that explain broadly what content stays up on the platform and what should come down. In May we went one step further and published the internal guidelines which we use to enforce those standards. These make clear why and how we reach decisions about what content should remain on the platform. They are available here www.facebook.com/communitystandards.

- At the same time, we announced that we will offer individuals the ability to appeal our decision if their content is taken down. Initially, this will cover posts that were removed for nudity / sexual activity, hate speech or graphic violence. We are working to extend this process further, by supporting more violation types, giving people the opportunity to provide more context that could help us make the right decision, and making appeals available not just for content that was taken down, but also for content that was reported and left up.

- On the 15th of May we published a new, expanded transparency report (https://transparency.facebook.com/community-standards-enforcement) which covers our enforcement efforts between October 2017 and March 2018 and covers six areas: graphic violence, adult nudity and sexual activity, terrorist propaganda, hate speech, spam, and fake accounts. The numbers show you:

  - How much content people saw that violates our standards;
  - How much content we removed; and
  - How much content we detected proactively using our technology — before people who use Facebook reported it.

Key statistics from the report include that

- In Q1 2018 we took action on 1.9 million pieces of ISIS and al-Qaeda content, about twice as much in the previous quarter

- We took down 837 million pieces of spam in Q1 2018 — nearly 100% of which we found and flagged before anyone reported it;

- The key to fighting spam is taking down the fake accounts that spread it. In Q1, we disabled about 583 million fake accounts — most of which were disabled within minutes of registration. This is in addition to the millions of fake account attempts we prevent daily from ever registering with Facebook. Overall, we estimate that around 3 to 4% of the active Facebook accounts on the site during this time period were still fake.

In terms of other types of violating content:

- We took down 21 million pieces of adult nudity and sexual activity in Q1 2018 — 96% of which was found and flagged by our technology before it was reported. Overall, we estimate that out of every 10,000 pieces of content viewed on Facebook, 7 to 9 views (0.07%-0.09%) were of content that violated our adult nudity and pornography standards.

- For graphic violence, we took down or applied warning labels to about 3.5 million pieces of violent content in Q1 2018 — 86% of which was identified by our technology before it was reported to Facebook.

- For hate speech, our technology still doesn't work that well given the need for context to judge what hate speech is and isn't. As a result content needs to be checked by our review teams. We removed 2.5 million pieces of hate speech in Q1 2018 — 38% of which was flagged by our technology.

Facebook have also developed partnerships with third parties to ensure our platform is as safe as possible - and we work with different organisations depending on this issue. For example, Facebook was a leader in setting up the industry-led Global Internet Forum to Counter Terrorism (GIFCT). Through this forum we are working with industry partners on technical pillars, such as a shared "hash" database – where content removed from one platform is shared between GIFCT partners, so it can be immediately removed or prevented from reaching another platform. Other companies that have joined the hash sharing consortium include GIFCT leads YouTube, Microsoft and Twitter, as well as smaller companies such as justpaste.it, Ask.fm, Snap, Yellw, Reddit, LinkedIn, Instagram, Oath and Cloudinary.

Regarding child online safety, last year we announced a joint progamme with Childnet and the Diana Award to offer every secondary school in the UK a trained digital safety ambassador. As many as 26,200 secondary school students and 2,000 teaching staff from 2,400 schools across the UK could be trained as Anti-bullying Ambassadors or Digital Leaders over the next two years.

Facebook have looked to build on our leadership in online safety by taking a significant role in defining standards on content and minimum standards more widely. We have taken an active role in establishing several existing codes of practice to ensure that minimum standards are set across different platforms. These include the UKICCS guidelines, the Royal Foundation's recent code of practice, and EU codes of conduct.

We have also indicated that we are very happy to work with Government and policymakers to develop standards for a Government led voluntary code of practice for social media companies. Potential areas where we could work together to identify standards include reporting and take down of content; terms of service/community standards; working with law enforcement; privacy advice and support; support for parents and carers; special tools for under 18s; and safety by design.

Social media has allowed users to be put in touch with news and information they care about. However, this has recently been abused by bad actors who want to spread misinformation for political or financial purposes. We are taking significant measures to combat this - but want to draw attention to two particular initiatives.

Firstly, in addition to measures to combat fake news we are already running in the UK, later this year we will begin partnering with third-party fact checkers to help improve the quality of content in people's News Feeds. If our partners assess that a piece of news being shared on Facebook is false, we down-rank it so that the audience for it will be much reduced.

Secondly, we are acting to prevent abuse of advertising for political reasons. Last October, we announced that only authorized advertisers will be able to run electoral ads on Facebook or Instagram. We have now extended that requirement to anyone who wants to show adverts about political issues on our platform. To get authorized by Facebook, advertisers will need to confirm their identity and location. Advertisers will be prohibited from running political ads — electoral or issue-based — until they are authorized.

We also announced that people who manage Pages with large numbers of followers will need to be verified. This will make it much harder for people to administer a Page using a fake account, which is strictly against our policies. We announced that political ads will be clearly labelled in the top left corner as "Political Ad" with "paid for by" information next to it. We've also been testing a new feature called view ads that lets you see the ads a Page is running — even if they are not in your News Feed. This applies to all advertiser Pages on Facebook — not just Pages running political ads. We plan to launch this globally in June.

We have developed the above policies, tools and partnerships ahead of regulatory action because we believe we have an important responsibility for the behaviour and content on our services. Our work in this area is ongoing, but we believe that we have made significant progress in recent months with industry leading product changes.

Data and algorithms

6. What information should platforms provide to users about the use of their personal data?

At Facebook we absolutely recognise the need to ensure users know what personal data is held by Facebook and have the ability to easily request that any item of data they no longer want to be held can be deleted.
In recent weeks we have introduced measures to make more clear the existing tools that users have to control their data and provided details of the further steps we are taking in this area.

In March 2018, we announced new Settings and Privacy Shortcuts and rolled these out for users in April. Our expanded tools for accessing information will allow users to see their data, delete it, and easily download and export it. We've also updated our Activity Log on mobile to make it easier for people to see the information they've shared with Facebook from their mobile device. More information on these developments can be found here https://newsroom.fb.com/news/2018/03/privacy-shortcuts/

In line with the GDPR, in April we began rolling out new privacy experiences for everyone on Facebook, which included updates to our terms and data policy. Everyone on Facebook will be asked to review important information about how Facebook uses data and make choices about their privacy on Facebook. We are rolling this out in Europe first but it will be available for every user on Facebook. More information on this initiative can be found here https://newsroom.fb.com/news/2018/04/new-privacy-protections/

Additionally, we have recently announced plans to build a new tool called "Clear History". This feature will enable users to see the websites and apps that send Facebook information when a user interacts with them, to delete this information from their account, and to turn off our ability to store it associated with the users account in future. If a user Clears History or uses the new setting, we'll remove identifying information so the history of the websites and apps a user has interacted with won't be associated with their account.

7. In what ways should online platforms be more transparent about their business practices - for example in their use of algorithms

At Facebook, we use algorithms to improve our products, offer customized user experiences, and help us achieve our mission of building a global and informed community. Of note, we use algorithms to help organize the content people choose to see in their News Feed (by "friending" someone or following a Page or joining a Group). As a company, when we think about improving our algorithms, including those that support News Feed, we are focused on three important principles: increasing transparency, non-discrimination, and increasing user control over their experiences. Reflecting these principles, we have a number of efforts underway:

- **We are publishing more information about how our algorithms work.** For example, we publish a series of blog posts called News Feed FYI that explains how News Feed works, highlights major updates to News Feed and details the thinking behind them. We also recently launched a new website feature called "Inside Feed' that provides an even deeper dive into the way systems work and the way to evaluate changes.

- **We are increasing users' control over their experience.** On News Feed, users have total control over who they choose to friend and follow — that's what determines what's in their News Feed — but there's also a tool to let users select people to "See First" so they are always at the top of their Feed. We are committed to building more such controls in the future.

- **We are promoting a series of AI educational initiatives and campaigns** to help people learn about the technology that underlies our various products and features, which includes AI and Machine Learning. A good example of this is the video that our FAIR (Facebook Artificial Intelligence Research) Lab published to explain what Machine Learning algorithms are and how we use them at Facebook.

- **We are working with external stakeholders on the ethical issues raised by algorithms and AI.** We are part of various multistakeholder consortia working on issues of algorithmic fairness, transparency and accountability, and this work informs our internal development processes.

- **We have a dedicated team working specifically on the intersection of AI & Ethics**. This includes conducting research and study into the ethical questions posed by AI, namely transparency and explainability, but also fairness, discrimination, etc.

Platform diversity

8. What is the impact of the dominance of a small number of online platforms in certain online markets?

What we see today is a very dynamic and innovative industry where stakeholders have an enormous amount of choice and there are constant new opportunities. We are committed to seeing a healthy ecosystem which will continue to flourish.

For example, there's considerable evidence that shows that it's actually never been easier for a startup to establish itself. A constant influx of new entrants is greatly facilitated by easy access to, among other things: (i) necessary infrastructure, available at no or low cost - e.g. there are a host of choices to rent—rather than build or buy—data centers, networks, storage etc.; and (ii) access to a large number of potential customers through the mobile application platforms and stores. Just by way of example, there are many tools that people can use to connect with others. Hundreds of popular messaging services and photo and video sharing apps are available, free to use and readily available.

- When someone wants to share a photo or video, for example, there's not only Facebook, but also - just by way of example - Snapchat, YouTube, Flickr, Twitter, Google Photos, and Pinterest.

- If you are looking to message someone there's LinkedIn, Apple’s iMessage, Telegram, Line, Viber, WeChat and Snapchat, not to mention traditional text messaging services via your mobile phone carrier.

When people decide to use Facebook, they often do it side-by-side with these other free apps.

Similarly, the advertising industry is fiercely competitive and we compete for advertising spend not just with a large number of other digital platforms, like Google, Amazon, Snap and Twitter, but also with offline media such as TV, radio and print.

Moreover, it is important not to lose sight of the considerable benefits which our users get from the platform and which promote a healthy ecosystem. Research has shown that across six countries that were surveyed in Europe (including the

UK) benefits include, (i) 49% of Small and Medium Businesses (***SMBs***) on Facebook say that they have been able to hire more employees due to growth since joining Facebook, (ii) 57% of SMBs on Facebook say that they have increased sales because of the platform, and (iii) 71% of SMBs on the platform say that the platform helps them attract customers.

In short, our platform helps small businesses across the world - particularly here in the UK - grow and create jobs.

European Union

9. What effect will the United Kingdom leaving the European Union have on the regulation of the internet

There are still questions to be answered regarding future regulation once Britain has left the European Union and the Government has stated that the UK will look again at the rules and regulations that govern the internet economy in Britain.

We welcome the Government's thoughtful approach to platform liability post-Brexit in their response to the Internet Safety Strategy consultation and look forward to discussing these issues as part of the White paper process.

The UK tech sector as a whole will benefit from UK data regulation that ensures adequacy with EU laws, which we hope will be achieved through the Data Protection Bill. The UK Government has said they want the 'one stop shop' feature of the GDPR to continue to apply to the UK post Brexit. It is important to note that this will mean - in the case of data protection law at least - that companies like Facebook would still be regulated by a lead regulator that was not necessarily in the UK, in our case the Irish Data Protection Commissioner. This would be a consequence of UK companies still being able to trade in the EU with their lead regulator being in the UK.

May 2018

Facebook UK, Google UK and Microsoft UK – oral evidence (QQ 174-182)

Tuesday 30 October 2018

Watch the meeting

Members present: Lord Gilbert of Panteg (The Chairman); Lord Allen of Kensington; Baroness Bertin; Baroness Bonham-Carter of Yarnbury; The Lord Bishop of Chelmsford; Baroness Chisholm of Owlpen; Lord Colville of Culross; Lord Goodlad; Lord Gordon of Strathblane; Baroness Kidron; Baroness McIntosh of Hudnall; Baroness Quin.

Evidence Session No. 20 Heard in Public Questions 174 - 182

Examination of witnesses

Hugh Milward, Director of Corporate, Legal and External Affairs, Microsoft; Katie O'Donovan, Public Policy Manager, UK, Google; Rebecca Stimson, Head of Public Policy, UK, Facebook.

Q174 **The Chairman:** Good afternoon. May I welcome our witnesses to this session of the House of Lords Communications Committee on our inquiry into internet regulation? Our witnesses are Rebecca Stimson, Katie O'Donovan and Hugh Milward, and I will ask them to introduce themselves in a moment. I would remind you that we are recording today's session. It will be broadcast online and a transcript will be prepared. There is the possibility of a Division this afternoon and, if that occurs, we will briefly suspend the meeting and resume after 10 to 15 minutes.

May I ask our witnesses from the tech giants briefly to introduce themselves and tell us a bit about the perspectives of their organisations? In doing that, perhaps they would answer a couple of initial questions. What are the advantages and disadvantages of the current regulatory framework for the internet as it affects your businesses and society? Also, may I ask our witnesses for their reactions to the Chancellor's announcement yesterday of a digital services tax, which is clearly targeted at the businesses that our witnesses represent? Perhaps we can start with Rebecca Stimson.

Rebecca Stimson: I am head of public policy for Facebook in the UK. I have been with Facebook for coming up to a year. I was a civil servant in the UK for 20 years prior to that, most recently in the Ministry of Justice. I do not have an opening statement other than to say I am very happy to be here as part of this very important inquiry.

Your first question was about the advantages and disadvantages and I think the advantages of the current framework are pretty clear. The UK has quite a thriving digital economy. It attracts an enormous amount of tech investment. It has an admired regulatory framework that applies to all our companies in various different ways. The evidence speaks for itself, if we think about consumers and the amount of choice they have, and the different platforms that they are able to use and engage with. What we see suggests that the framework is working extremely well.

I am sure we will come on to some of the disadvantages in the questions around how that framework can keep pace with change. Having done some work on GDPR in my old life as a civil servant, I know how complicated it is to write something that is future-proofed.

In answer to your tax question from yesterday, we are in the process of looking at exactly what the Chancellor proposed, and we need to see it in detail, but there is a consultation document expected very soon, as I understand it, and we will be fully engaging with that process when we see it.

Katie O'Donovan: I am UK public policy manager at Google with responsibility for a number of our policy areas in the UK. I also sit on the board of the Internet Watch Foundation. I mention that as it may come up in the course of the conversation.

Thank you very much for inviting us to give evidence today. We have been following your inquiry with interest. We recognise that this is a time where people are thinking more and more about how they use technology in their daily lives and, indeed, whether regulation has kept pace and whether there are areas to explore within those conversations. While Google is institutionally very young—we recently turned 20—as a technology company, we are one of the oldest. That gives us a perspective from which to see how our products have evolved over time, how the use from users has changed over time, and whether we need to change the way that we exist and operate.

In terms of the benefits and shortcomings of the current situation, there are inherent benefits in the way we are able to access the internet online in the UK, and sometimes we skip too quickly over them. We have the ability to access information from across the world in almost real time. A school child in India and a professor in Oxford now have the same ability to find out crucial information, to stay in touch with friends and family from around the world and to start businesses and exporting, in a way that was impossible to think of 10 or 15 years ago. It is well worth contemplating that and preserving it.

As I reflected earlier, the way that we all use the internet in our daily lives, the way that young people and companies use the internet has changed quite dramatically. We have changed and evolved as a company. We have been able to address some of the issues in the way we work without waiting for regulation. If you think about the way that we deal with very serious issues such as child sex abuse imagery, we have been able to work in partnership with institutions such as the Internet Watch Foundation. We also work very closely with the Government and other bodies when there are issues that require specific regulation. It is an inquiry that we are very happy to participate in and we have learned a lot from the evidence of your other sessions, too.

On the question of the Budget yesterday, we also saw the Chancellor's proposal and are waiting for the consultation document. We very clearly understand the importance of the tax issue and the policy discussions and scrutiny that have come under that. The Chancellor referred to his proposals as part of setting a timeline for international action and we have always supported that. For a tech company such as ours, and indeed for many other companies that operate across borders in different countries, a multilateral international solution would be really meaningful and of long-term significance. We continue to support an international resolution to these issues.

The Chairman: Hugh Milward.

Hugh Milward: I run corporate, external and legal affairs for Microsoft, but I am not a lawyer. I want to make that really clear. Microsoft seems to be one of the elder statesmen of technology companies. We are nearly 45 years old and we have seen a few battles over the years. Some of these issues have arisen before and we are very keen to participate in your Committee and try to offer what we can from the experience we have gleaned over the years.

The opportunities that technology affords society are tremendous and very significant, especially with the advent of AI, something that we are developing at pace. The biggest worry that we have is around the trust that society has in technology. We believe firmly that if society does not trust the technology, it will not the use it, and will not benefit from the opportunities that technology provides. It is incredibly important that we get this right and ensure there is a high level of trust across society, and that we come together as the technology industry in committees such as this, and with government and civil society, to navigate our way through some of these very complex issues. These issues are developing at pace and in real time and we are trying to find ways in which to solve a series of issues that society is concerned about.

At the heart of it is how we make sure that society can trust the technology that is going to benefit them so much. We do not feel that there is a Wild West of unregulated space at the moment. In fact, there are a range of regulations in place which help to provide that level of trust. If you look at laws governing connectivity, intellectual property, copyright, net neutrality, data protection, privacy, advertising standards, et cetera, these are all regulations and laws that already affect technology companies. Generally, if a law applies offline it applies online as well. It is not really the Wild West that it is sometimes painted. There are some very specific examples of quite new regulations or voluntary measures that are working extremely well, which we can go into in due course.

In terms of a digital tax, again we are digesting what it was that the Chancellor announced yesterday. It certainly looks to be interesting. What remains to be seen is how this would dovetail with what the OECD is driving at. Probably the most important thing is how this influences what the OECD is thinking and how the OECD influences what the Chancellor decides to do. We will respond to the consultation, as the others have said.

Q175 **Lord Allen of Kensington:** I would like to stick with tax. I completely understand you saying that you need to understand the detail, but my question is more philosophical, in that to be trusted, as you said, Hugh, and to be a good corporate citizen, frankly, tax is a big issue, whether in the pub or in Parliament, and people do not understand why you are taking so much revenue from the UK and you are paying so little tax because of clever tax schemes. You might say that you are paying what you are asked to pay, but that does not feel like you acting as a trusted good corporate citizen. I would like your views not on the detail of the tax but that specific point, because it is a massive issue. A number of people who have given evidence have raised that. The second point, and related to that, is whether 2% is equitable versus what non-digital companies pay; does that feel equitable? The third thing is a number of people have said, whether it is a tax or a levy, something could be used to help fund the regulation of the internet. I should like your views on those three points.

Rebecca Stimson: We all recognise that tax is quite a sensitive issue and, as you would expect me to, I would say that we pay all the taxes in the UK that we are required to pay. In recognition of your point that people look at the turnovers of these companies and have questions about the tax regime, I am sure you are aware that Facebook made a change in 2016 to move more to a local-seller model to increase the amount of tax that we pay in the UK.

Lord Allen of Kensington: What percentage of your turnover is paid in tax?

Rebecca Stimson: I would have to check that figure. I do not know that figure off the top of my head, I am afraid. To your point about a levy, I can again understand why people might look at companies such as Facebook and say, "We should get them to pay a levy". That is not an idea that we would automatically be against, but, as you have heard from previous witnesses, and certainly from the way the Government are approaching this whole area, we need to think about what you are trying to do and the harms you are trying to tackle. Recently, the head of the NHS, for example, called for a levy to address the impact on mental health of social media. We would need to begin by looking at the evidence, scoping that problem and defining the harms, and work through to whether it is clear that a levy on social media companies would be the most effective way forward.

Katie O'Donovan: You are absolutely right that this is an issue that consumes people whether they are in a pub or in Parliament and they often want to discuss it. We also pay all the tax that we are due to pay in the UK and that has increased over the years. The question is about how we pay the tax as a proportion globally. We are a US-founded company which is headquartered in the US, and so our global tax rate over the last decade has been 26%, which is comparable to UK corporation tax, but the proportion we pay in the US as our home country is 80%. We think it is important to have an international resolution to this tax issue so that the issue is not solved in one country but has knock-on consequences in other countries.

Hugh Milward: Likewise, we pay all the tax that we owe in the UK, as we should. Before we start looking at a levy to fund the regulation of the internet, we would probably want to go back to thinking about what kinds of interventions are required to get the desired outcomes through regulation of the internet, and look at how we design that to solve the problems that we are trying to solve; and then look at whether a regulator is the right approach and how we would fund a regulator, rather than doing it the other way round.

Lord Allen of Kensington: I would ask the same question of Katie about funding regulation. I would also ask each organisation what percentage of turnover is paid in tax in the UK. You might need to come back to us.

Hugh Milward: I will need to come back to you on that.

Katie O'Donovan: The tax we pay on our profits globally is 26%.

Lord Allen of Kensington: I am talking about tax in the UK as a percentage of turnover.

Katie O'Donovan: We can come back to you on that.

The Chairman: We will write to all three of you and ask you to tell us the amount of tax that you pay in the UK as a percentage of your turnover in the UK.

Katie O'Donovan: That is not generally how tax is calculated.

Lord Allen of Kensington: I understand that, but I am trying to understand how equitable it is versus other offline companies. Katie, you were going to come back on funding regulation.

Katie O'Donovan: You asked about a levy. Rebecca mentioned one example but there are lots of different areas where, in recent times, a levy has been suggested to pay for whether it is a regulator or a particular part of the service. Indeed, the Government's Green Paper on the internet safety strategy suggested a levy around educational services for online safety for children. We have discussed this with the Government. In that particular instance, we invested millions of pounds in our own education programme. We have a programme called Internet Legends, and one for teenagers called Be Internet Citizens, which reach hundreds of thousands of young people each year. To build on Hugh's point, we need to have a very specific point of reference for what a regulator would do or what the levy would be required to do, and if that is the most effective way to do it. It is certainly a conversation that we are very happy to continue with government.

The Chairman: Baroness Quin and then we will move on to market concentration.

Q176 **Baroness Quin:** Hugh mentioned trust and that is an important theme that runs through a lot of the work that we have been doing here. Does each of your companies operate under a set of guiding principles for how you deal with customers and how such principles can strike a balance between your desire to get as much information from customers as possible and, at the same time, respect the desire of customers not to want to have too much information about them being divulged or accumulated? If you have such guiding principles, are they made public or are they discussed between the main companies which are operating? How do you interact with, say, other people who have given evidence, such as Which? or Doteveryone, in terms of addressing their concerns? I know those are wide-ranging questions, but could you at least make a start on the guiding principles and what this means for users and people who are concerned about users?

Rebecca Stimson: We want Facebook to be a safe and enjoyable place where all the people who sign up to use it get a positive experience to connect with the people who mean something to them—their friends and family. There are a whole host of guiding principles that we operate under depending on what aspect of the business you are talking about. It can be anything from ensuring that our policies are very clear and accessible to people, so things such as data privacy and what we do with your information, to educational material about how to be safe online. We have a number of different ways that we engage with parents, teachers and younger people to try to drive up digital literacy and awareness. Sometimes that is the quite practical basics of understanding how to do certain things on our platform. We try to design our tools so they are intuitive and easy for people to use. You referenced people's information, and the way it is framed and reflected in regulation is that people's data is theirs. They can control it, move it around, set their privacy settings and manage their data on our platform with a whole range of tools that we provide. As I say, we embed the values of our company into the products that we make and we try, in a whole host of ways, to reflect that for the consumers who use them.

Katie O'Donovan: Google has a singular company mission, which is to make the world's information universally and usefully accessible. That guides everything that we do. We also have a very practical principle in that we put the user first in all the decisions that we make. To give you an idea of how that comes to life, when Google started as a search engine, the creators wanted to get people off the search engine as quickly as possible. One reason that Google was successful is that you could search for your answer and you knew with confidence that you could click on the blue link and it would take you to the site that you were looking for. Back when Google first started, other search engines created incentives for you to stay on the search page site. You sometimes had quizzes or crosswords or Sudoku alongside the search engine, because part of their business model was to keep you on their search engine site for as long as possible. We know we are doing our best as a search engine, and it is inherent to the users' experience that they know they can go to Google and within a fraction of a second they can click on the sites they want. That is not necessarily commercially viable. On the vast majority of searches we do not have advertising alongside because they are searches that people do not want to advertise against. On the searches where we believe there is a commercial attraction to advertise, or where people want to advertise, they can, and, of course, if somebody clicks on their link we receive advertising revenue from that.

By putting the customer and user first, we were able to build a fast and efficient search engine which was not monetised in every single search, but which did such a good job customers and users kept coming back to it. You mentioned Doteveryone and Which?. Which?, particularly, has a long history of understanding consumer rights and behaviour in the UK and Doteveryone has done some very interesting work in this area. To have a bit more granularity and understand a little more about how a search works, we published what we call our rater guidelines, which is a 160-page or so document, which is freely available on the internet to everyone. It is a set of guidelines we give to people who do quality control work on search engines to check that our algorithms are doing what is best for the user, best for the searcher, and makes the right decisions to return the right results. Those guidelines are available for anyone to look at and for a research organisation to fully scrutinise if it wants to.

Hugh Milward: We have a set of principles at the heart of our mission as well, which is about empowering everyone on the planet to achieve more.

Baroness Quin: Are those principles made public?

Hugh Milward: Yes. For the most part, the services that Microsoft offers are services that people pay for—Word, Excel, Powerpoint and a variety of others—and if you are looking at some of the more leading-edge services, in AI for example, again we are building a series of building blocks that customers use for their own purposes. Most enterprise customers use them for their own purposes and they pay us for it. We offer it in that way. In that sense, they see a direct value in the information and service they get, otherwise they would not buy it. That monetary exchange is very transparent.

The principles that we believe in around data, very similar to what my colleagues on the panel have said, are about it being the users' data and that they should have control over that data, determine what happens to it, where it goes, where it is located and how it is treated. That is a fundamental principle of the way in which we design and offer services for our customers.

Baroness Quin: I should have made clear a family interest in that my stepson works for Google. I take the points that you made in response. We seem to have come across a general perception that people are nervous about what data is held about them. It does not seem to them as transparent and as open as you have suggested. As a user myself, if I go online and am asked about cookies, for example, I tend to say, "Yes, that's all right", without thinking, because I want to get the information quickly, and I wonder afterwards whether I should have done that or not. Despite the good intentions of the principle, is there still a gap between what people know about the system and how to access their own data and so on; and despite the procedures that you put in place, is there a problem of users not being familiar with the ways that they can protect themselves?

Katie O'Donovan: Which? has done some research into this to show a disconnect between the information that is available around their data and how they understand it. For example, if you have a Google account, you can go on to something called My Account and it will show exactly what data we have and how we use it. You can choose how we use it and if you want us to understand where you are searching from, you can share that. If you do not, you can turn that off. Globally, we have had 2 million visits to that, which is an extraordinarily high number, and a positive measure for us to say that that is working.

We also see a very high number of people engaging with that. There absolutely is more that can be done to make us conscientious users of technology. One reason we have invested so heavily in primary and teenage education is to help people understand online literacy and begin to think more consciously and critically about how they share information, and in which cases that is beneficial and in which cases it is not.

Hugh Milward: An incredibly important principle lies behind this, which is that if you have an accident and an ambulance comes to pick you up and take you to a hospital that you have never been to before, you really hope that the medical practitioners who are going to be caring for you have access to your medical records and to other bits of information that you have previously given to the NHS, so that they can treat you in the best possible way. If the consumer, if society does not have—and I go back to my point about trust—a level of trust that allows the NHS to have that data to be able to use it for the benefit of patients, something has gone wrong.

It is incredibly important that we ensure that we separate out the different concerns people have about different types of data and the way that the data is used. It is a lot more nuanced than a simple, "Do we or do we not trust other entities of whatever kind with our data?", because there are several use cases where we can very clearly see how consumers would absolutely trust different entities with their data. I have nothing against the NHS at all, but the way the NHS is currently looking after data raises a lot of questions because its storage of data includes manila envelopes on trolleys in corridors. There is a lot further we can go and a lot of trust that we need to continue to build with the general public about the use of data that is not about stoking fears around data use.

The Chairman: Rebecca, do you wish to add anything?

Rebecca Stimson: No, I would reflect the same kinds of comments.

The Chairman: All three witnesses have referred to published guidelines or principles that they have. The Committee would welcome it if you could send what you have published and an indication of where you publish it and in what way it is available, and in what way you measure your conduct and performance against it. Baroness Chisholm.

Q177 **Baroness Chisholm of Owlpen:** Sir Tim Berners-Lee has expressed concerns that the world wide web has "evolved into an engine of inequity and division, swayed by powerful forces who use it for their own agendas". Are there any risks for consumers and citizens associated with the concentration of digital markets within the hands of a few large tech companies? If so, how might such risks be mitigated?

Katie O'Donovan: That reflection is really important and one that we should—and do—consider very carefully. The way that we all use the internet now is very different from how we used it 20 years ago, and it continues to change. I do not recognise the characterisation of concentration of the digital market in the way that it is commonly portrayed. We have a very clear mission as a company and we operate with great transparency on this. The way that we add value to people in the UK can be measured at an economic value of around £50 billion. That economic value, the low barriers to entry and the innovation that the internet is able to provide are worth reflecting on. There is also a highly competitive market online because of those low barriers to entry. I talked a little about how searches evolved from 20 years ago, when we first started, and even today, around a quarter of searches are brand new; they are for information that people were not looking for yesterday or are looking for in a distinctly different way.

That provides us with an enormous challenge. Even if everything else had stayed still, we need innovation to take us from where our search engine was 20 years ago, when the amount of information on the web was akin to a big city or university library, to the exponential growth of information today, where users not only require search results as quickly as they did 20 years but they want them from their mobile phone or they want to use voice or they want something else. That change in technology and in consumers' expectations delivers innovation in our markets. In the markets that Google operates in in the UK, when people go online to buy something, 50% of those journeys start on Amazon. We are competing with travel organisations for flight information and other video platforms which are launching, and there is a real vibrancy to that.

Over the 20 years that Google has existed, companies have been at the top of their game and then fallen away. The prominence of certain companies at a certain time does not reflect a lack of innovation in that space or a certainty over what will happen going forward. We thrive on innovation and feel we are operating in a very competitive environment.

Rebecca Stimson: I would reflect that very much. To use Katie's words of a thriving digital economy in the UK, while there are bigger and smaller players, if you think about it from a consumer perspective, and I am sure I read recently that on average people have 80 apps on their phone—I do not but apparently people do—it has never been easier to start up these kinds of businesses. In the time that Facebook has existed, other multimillion-dollar international companies have either grown alongside us, such as Twitter, or grown with us, such as Spotify. There are tens of millions of UK businesses that operate successfully through our platform. Part of the regulatory framework now—to reflect the previous question—concerns the fact that the data that flows around to enable that is the users' data, and it is theirs to move around. If I think about my own phone, I give my data to numerous apps that I use on that phone. It is not the preserve of any one company, irrespective of its size in the market. I would echo what Katie has said, that the premise of the question is certainly not our experience of being in a very competitive market at the moment.

Hugh Milward: The only thing I would add is that the increasing trajectory of digitisation in the economy means that pretty much every company is a tech company, or should be a tech company within a few years. In that kind of market you have to look again at what you mean by competition. What does dominance look like? If you look at operating systems, for example, around 10 years ago we went from a market penetration of 90%-odd down to around 14% of the install base, and that is because of the arrival of a whole variety of different competitor operating systems which fundamentally changed the market. That was over a nine-month period. You see these fundamental shifts in the way that we think about what competition looks like, and with the level of digitisation across all major companies in the UK economy now, we think pretty much every company will be a tech company, and that will mean big changes and a lot of competition in the marketplace.

Baroness Bonham-Carter of Yarnbury: I take the point that there are bigger and smaller players, but there are the really huge players that you all represent. What are the implications of such a tiny number of companies acting as gatekeepers to the internet? We heard from the Information Commissioner that she was concerned at the "pervasiveness of big data analytics and micro targeting. These concerns are magnified by mergers and acquisitions where personal data is the primary asset".

Rebecca Stimson: Partly I would go back to something I said previously, which is that I would look at this from the consumers' perspective. We have a very robust and well-established competition law framework and regulatory framework in this country and, if you think about how they approach these things, they look at the conduct of the companies and whether they are abusing their market position.

Baroness Bonham-Carter of Yarnbury: Who does?

Rebecca Stimson: The competition authorities.

Baroness Bonham-Carter of Yarnbury: Sorry, I thought you were talking about the consumer.

Rebecca Stimson: Not yet. They look at whether we are abusing our market position, whether we are a barrier to entry, whether we are upholding proper standards of ethics of safety around users' data, whether consumers have lots of choice. As far as I am aware, the relevant authorities in the UK are satisfied that that is what this digital economy looks like in the UK at the moment. As I have said, people worry about data being concentrated in particular companies, but, to reflect Hugh's point, the way that the markets are evolving means that data is shared by consumers with all kinds of different companies, from a supermarket online, to a social media app, to Uber, to something else, and it is not the preserve of those companies to hold it or fence it away from anyone; you can move it around as much as you like. I would approach the question in that sense, thinking about competition regulation as it stands at the moment, the way in which it comes at it from a consumer perspective and the very positive picture there is in the UK at the moment.

Baroness Bonham-Carter of Yarnbury: So you do not accept the Information Commissioner's concerns.

Rebecca Stimson: I think the Information Commissioner was talking about micro targeting; is that correct?

Baroness Bonham-Carter of Yarnbury: Yes, which is quite an important element in this.

Rebecca Stimson: I understand that as being a slightly different question from competition—and please tell me if I have misunderstood that. That is about how messages, campaigns and advertising target people online.

Baroness Bonham-Carter of Yarnbury: That was my question.

Rebecca Stimson: Apologies if I misunderstood your question. People are very interested in the issue of how advertising is targeted online. At Facebook we have been quite transparent about how our algorithm operates to inform what people see in their newsfeed. As I am sure you saw, this is a particular issue when it comes to political advertising, and we made a change, I believe it was last week, that, going forward, all political adverts have to be labelled as such and it has to be clear who is paying for them. We have done that in advance of a consultation the Cabinet Office is currently doing on the same kinds of reforms to electoral law, particularly in the space of advertising. We have already made a change in advance of that consultation.

Katie O'Donovan: On concentration of data, to reflect on some of those points, data is not a limited asset. It is not like a physical property. To tackle a phrase that is often used, it is not like oil that only one person can use and own. People control it themselves, and that has been strengthened by the GDPR, and certainly, as a company, we never sell data to any other company. We empower our users to manage their own data. Another thing that is relevant to how we operate as a company is the technology and methodology that we use on data that adds the value and enables us to offer services that people keep asking to use. As Hugh mentioned earlier, the use of artificial intelligence has become increasingly important in our work and, as such, over the course of the last couple of years we have re-trained all our engineers so they can be artificial intelligence-based in their approach to topics.

Baroness Bonham-Carter of Yarnbury: That does not fill me with great confidence, I have to say.

Katie O'Donovan: AI suffers from the fact that it can be portrayed in a way that is geeky and fantastical—the stuff of futures, but not necessarily the futures that all of us would like. In practical terms, however, it can really help people. We use it in maps to help us understand if it is quicker to go from here by walking up to Tottenham Court Road or to get on the Northern line and leave at Charing Cross.

Baroness Bonham-Carter of Yarnbury: Katie, does it not send people deeper and deeper into where they are wanting to be sent rather than expanding?

Katie O'Donovan: Not at all. The way we use artificial intelligence is to enable users to perform the tasks they want to do quicker and more effectively. We have developed our own AI principles to ensure that we use them ethically, that we have transparency about them and that we use them for social good. It is important to say that AI could be misrepresented as being able to be used for sinister ends, but it is a practical technology that can be used positively.

My point was that as we have increased our capability in artificial intelligence as a company, we have made that publicly available and open source, so that engineers from other companies, whether they are competitors or not, or a computer studies student in their bedroom, can access TensorFlow, which is our open source artificial intelligence, and build their own programs from that. We are not keeping that technology to ourselves. We are broadening the whole ecosystem with that. It is an incredibly popular service that we offer on the open web.

Hugh Milward: Along the same lines, we are designing for others to use rather than for us to use. It is a slightly different model, I guess. There are different types of data and, as has previously been mentioned, there is very little data that is unique and proprietary and cannot be replicated easily anywhere else. For the vast majority of data you can create observed or inferred datasets quite easily, and that results in very low barriers to entry for new market entrants. That is one of the tests that competition authorities look at. In those situations where there are unique datasets, and where there is no substitute for them, it is right that the competition authorities look at that and test whether it is a barrier to competition.

The Chairman: May I ask a question on competition more generally? Which? says that many users of your services regard you as utility services that they cannot do without. Do you therefore understand why it is argued that you should be regulated as utilities?

Hugh Milward: Users quite like Word, Outlook and various things, but there are free versions of everything we offer, and when they decide to pay for another year’s subscription, they do so in the knowledge that there are a lot of free alternatives. I think the market is working well there. If there is a dominance of Word, Outlook and other things, it is a dominance because people choose it again and again.

The Chairman: Do you see yourselves as a utility provider?

Katie O'Donovan: No, I do not think we do, because there is a real choice. Every time people go online, there are rival search engines that have grown phenomenally over recent years, operating in a different way from us. As I mentioned earlier, the majority of online shopping activity starts on a different site from ours. With such low barriers to entry and the ease with which consumers are able to move from one to another, we strive and work incredibly hard to ensure that we are the search engine that people come back to. Hugh’s point earlier that the dynamics of the online environment can shift in a matter of months is worth dwelling on because that is how consumers will use us. If we are useful they will hopefully keep returning.

The Chairman: Rebecca, do you see yourselves as a dominant utility?

Rebecca Stimson: No, I do not think so, and I would reflect similar comments, in that if you think about things people use Facebook for, such as messaging each other, sharing photographs, looking at news online and so on, there is an enormous range of other companies and platforms that will enable you to do those things, so, no, I do think I would recognise that.

The Chairman: Nonetheless consumers do. Baroness Chisholm.

Q178 **Baroness Chisholm of Owlpen:** Do you think there should be a public interest test in mergers between businesses which rely on user data?

Katie O'Donovan: I am not an expert in what already exists in terms of public interest tests in mergers. I believe we have a very robust system here, but I would need to get back to you on that one.

Rebecca Stimson: As I said in my previous answer, the competition regulations here are very stringent and thorough, and I am sure that kind of test must exist. I am not an expert in it, but these kinds of mergers and acquisitions are happening in this marketplace under the full scrutiny of the current UK regime.

Lord Gordon of Strathblane: The point is if you take media mergers, there is not simply an economic test; there is a public interest test as well as to whether it is a good idea for society that it should happen. The simple question is: would that be a good idea in the field of your companies?

Hugh Milward: In which market? Part of the challenge is to define what the market is.

Lord Gordon of Strathblane: I accept the problems but, on the other hand, we have been told before that Google has a 94% market share in the UK.

Katie O'Donovan: I do not think that is accurate. I think Microsoft would challenge that statistic.

Hugh Milward: We have at least 12%.

Baroness McIntosh of Hudnall: I want to reframe this question, if I may, Chairman, about the utility issue, because each of you answered as if you were being asked whether your company is a utility. That is not really the question. The question is whether access to the internet is a utility. It is quite obviously the case that electricity is regarded as a utility. There are many companies operating competitively within that market, but it is regulated as a utility for reasons to do with public interest and the public good. Could you very briefly answer the question again in relation to access to the internet as analogous to access to clean water or electricity or any other utility you can think of?

Katie O'Donovan: In the UK, access to the internet is often provided not by the companies here today but by telecommunications companies, and I believe there are statutory duties on them. I am not looking to obfuscate and avoid answering your question, I am just saying that we are not responsible for the access to the internet in the UK.

Baroness McIntosh of Hudnall: I am not asking what you are responsible for; I am asking about an issue of principle and what your view is.

Katie O'Donovan: The Government themselves have said that access to the internet is of inherent value to UK citizens. They have their own standards and expectations for the speed at which that should be delivered and the availability of that in rural areas and elsewhere. As a company which relies on internet access, that is absolutely welcomed. If you are asking more broadly if should there be regulation in this space, or of what our companies do, that is a slightly different question, which I am very happy to get into a discussion on.

The Chairman: If only we had the time. Do the other witnesses wish to add? No. Baroness Bertin.

Q179 **Baroness Bertin:** I should first declare that I work for BT. I would like to talk a little about content and user-generated harms. I would kick off by asking what responsibilities do you have in terms of moderating user-generated content?

Rebecca Stimson: Obviously some of this is covered by the existing regulatory framework, including by the e-commerce directive, where we have a liability, as I am sure you are aware, for illegal content online. There are other things that apply to content such as data protection, GDPR and so on. As I am sure colleagues here have, we have a broader sense of where our responsibilities lie. That is best demonstrated by our content standards, which are very extensive documents on what we do and do not allow on the platform, which are public, so that people can see and understand those. They concern a whole range of different issues, from things such as sexual exploitation images, to bullying, terrorist content, nudity.

Baroness Bertin: If I can stop you there. You know all the figures—the NSPCC has published them—and we still have terrible figures. Some 25% of children have seen content on Facebook and YouTube that contains suicide, and I could go on. Something is not quite right yet, is it, especially in terms of protecting children online?

Rebecca Stimson: I would recognise that there is always more we can do. I am not going to sit here and say it is all fine because it clearly is not. The statistics show that the overwhelming majority of people who engage with Facebook have a positive experience and see good things but, while there are people who see bad things, there is more for us to do.

Baroness Bertin: Sure, but it is about priorities, is it not? It is important to acknowledge that as an industry you have come together and done good work on terrorism, for example, but—and correct me if you think this is wrong—from speaking to law enforcement agencies, it feels that the child protection element is a rather hard yard, if you do not mind me saying. I would love to know how high up your list of priorities this issue is in your companies, how much time is spent on it and how much brain bandwidth you are giving to putting in new ethical designs to change the agenda, so that, for example, Katie, if I were to put in a multi-layered search I would not get category A child abuse images, which you still can get, I understand?

Katie O'Donovan: Can I start on answering that question? We have a very clear policy against any illegal child sex abuse material being discovered through search. I too have talked frequently with law enforcement agencies and have said to them that our algorithms are set not to return any of that content.

Baroness Bertin: But, as I understand it, you could do a repeated layered search and still get category A child abuse images.

Katie O'Donovan: I do not know what "repeated layered" means.

Baroness Bertin: This is the language the law enforcement agencies use and they say they have evidence you could still get those kinds of images.

Katie O'Donovan: I have talked very frequently to law enforcement agencies and made clear that our policy is not to deliver any content through search that is classified as child sex abuse, and, if they have information or instances where that is not working, to please let us know so that we can ensure that our services are working as well as possible.

To answer your broader question about how we collaborate on issues such as this, we are members of the Internet Watch Foundation, which is an organisation based in the UK. As I said earlier, I am on the board. It is a world-leading organisation, with over 100 members, technology companies, big and small, working together to tackle the issue of illegal child sex abuse imagery. For Google itself we have developed technology that not only uses hashes, which have been developed by Microsoft and others to identify known child sex abuse, but just six weeks ago, we announced that we have developed a review classifier which increases significantly the effectiveness of our human reviewers looking for this content for the first time to identify unknown child sex abuse imagery. It really is treated very seriously.

If we move on from illegal child sex abuse imagery, I think you also asked about issues of concern to young people, and, obviously, young people online can come across content that they are not ready to see or they do not want to see or it is inappropriate that they see, and, as well as having community guidelines on YouTube video-sharing platform that go above and beyond the law and are enforced through our flagging systems using technology, we have also invested really heavily in YouTube Kids, which is a platform for under-13s to access some of the user-generated content and some of the content people really like from YouTube but in a much safer and more relevant environment.

Baroness Bertin: To build on that, in terms of your investment and putting your not inconsiderable brain power into these issues, what percentage of R&D do you invest? Do you think it is high enough up the agenda in your boardrooms?

Katie O'Donovan: From the R&D we put into this, we know this is one of those areas where artificial intelligence can be hugely beneficial. We are able to use artificial intelligence that has been developed for a general purpose to help us identify content that we think may be child sex abuse imagery. In that case, that is changing the way we have been able to tackle this issue.

Baroness Bertin: Do you have a figure for your R&D?

Katie O'Donovan: The R&D that we use is developed for general purpose so we do not have one technology team here that works solely on this issue and another technology team over there. There is technology that is developed for a general purpose which can be utilised in different ways. That is a benefit to us. That means we can use software that is developed through commercial means to help us on these issues. We make sure we do because we realise we have the resources to invest a significant amount of money.

Baroness Bertin: You could completely change the game and solve a lot of these issues, I would have thought.

Katie O'Donovan: I would not necessarily claim that we could do that, but we have been able to invest really significant amounts of money and computational power. We developed video-hashing technology, which enables us to find content of videos which is known child sex abuse imagery. The development of that technology has required significant resources and investment and we are making it available to companies big and small. Microsoft and Google collaborate often on this topic, but we go beyond that to companies which could never begin to afford this technology. We take this really seriously. It is an incredibly difficult issue which we know requires an industry-wide response and the right policies and investment in technology, and we absolutely have made that.

Baroness Bertin: Obviously, you would never dream of selling a product that did not have anti-malware and antivirus programs. How much ethical design are you putting into your products? How much more thought will you be putting into horizon scanning going down the track?

Hugh Milward: There are different aspects of ethical design. For example, building accessibility into the fundamentals is fundamentally important. Going back to the drawing board of the use case of a particular product, it is about how you make sure that it is accessible to everybody. That is an ethical way of building a product. Hopefully, that is a given. It is not just about ethical design; it is also about how much effort is going into the development of these kinds of things. One of your questions a little earlier was implying that surely we can solve this if we put enough effort into it. The risk is that we lull ourselves into believing that is possible, but what happens is it just gets driven to the dark web and it becomes out of the control of all of the companies sitting at this table, and we have no control over the dark web. That is what happens.

All the companies here use PhotoDNA, which we spent a lot of time developing 20 years ago. We have just concluded a massive engineering project on VideoDNA. It was launched a couple of months ago, and we are hoping to use it in exactly the same way. It requires significant amounts of engineering effort to do that. It will produce cleaner and cleaner results the more we use it. The behaviours of those predatory paedophiles are not being addressed through the actions of those at this table. Their activities are being driven further and further to the fringes of what we have control over, and that means the dark web.

Baroness McIntosh of Hudnall: Shall we move on to the moderation point? It comes back from the issues of the dark web, which are outwith your control and, indeed, anyone's control at the moment. When you look at content uploaded on to your sites, you have ways of moderating it that include algorithmic methods, and, I imagine, humans. It has been put to us by more than one witness that the number of human moderators who are actively engaged in looking at content on your sites is very small compared with both the number of users and with the amount of algorithmic moderation that goes on. Do you think the balance is right between those different kinds of moderation and do you have any plans to extend them in any direction?

Rebecca Stimson: You are right that at the moment it is a balance of automated moderation and moderation by humans. The automated systems, as has been alluded to in the previous answer, are really good in some respects, such as for detecting terrorist material and child sexual exploitation. Some of the statistics that all of us are producing are very good. Recently, similar to Google, we announced our new tools for unknown child nudity images. They have an extremely high success rate. There are some more complicated areas such as bullying which still require human moderation. Sometimes it is about context and sometimes it is difficult. While we have a certain amount of automation to spot it, it often still requires a human being to review it. As you say, we are investing very heavily in the machine learning but it has to be accurate. We cannot have it misunderstanding what is happening and censoring large amounts of content unnecessarily. We have gone from 10,000 to 20,000 people working on safety and security in Facebook.

Baroness McIntosh of Hudnall: Is that world wide?

Rebecca Stimson: Yes, that is a global figure.

Baroness McIntosh of Hudnall: How many users do you have?

Rebecca Stimson: We have around 2 billion users. That is alongside the tens of millions of pieces of content that machine learning is able to look at in several of the most important areas.

The Chairman: Can you give the number of users in the UK? You have given the global number of users.

Rebecca Stimson: I believe the number of users in the UK is 40 million.

Baroness McIntosh of Hudnall: And how many moderators would be looking at that area?

Rebecca Stimson: The way that moderation works is we have teams around the world 24 hours a day, seven days a week. When people report content that requires moderation, there is not a UK team to look at UK content; it will be sent and will depend on what it is and whether it needs specialists to look at it or whether it is a matter for law enforcement. I am not able to give you the number of UK moderators for so many users.

The Chairman: Something as context driven as bullying, for example, probably needs a UK moderator to properly comprehend it. Is that right?

Rebecca Stimson: It depends. Hate speech is an example where more local knowledge can be helpful. We call them flows and that is where the different pieces of content being reported go to different places. I am afraid I could not give you a specific number of users and moderators in the UK because it does not work that way.

Baroness McIntosh of Hudnall: It would be quite helpful if you could give us some idea, given that, exactly as you say, context is everything with some of this stuff, and language is also very important, not just whether it is English or French, but whether it is English used in a different way. English is used in a different way here compared to America or Australia. If you could give us some notion of how local to the UK moderation and investigation of content on your site is, that would be very helpful.

Rebecca Stimson: I am very happy to try. As I said, it is not quite how that system works but let me come back to you with an answer.

Viscount Colville of Culross: We had evidence a few weeks ago about the number of moderators that you have in Germany compared to the number of moderators you have world wide. There is a hugely disproportionate number in Germany because of the law it has about hate crime. Is that not tempting legislators here to try to follow the same course to make sure you have more moderators?

Rebecca Stimson: I think you are referring to the netzDG law.

Viscount Colville of Culross: I am indeed.

Rebecca Stimson: I will take a moment to be clear about what that law involves. There are hate speech laws in Germany which almost entirely map across to our own hate speech rules whereby if something is reported to us we take it down. Some things in Germany are specific to Germany. The netzDG law required us to introduce a reporting mechanism so that people in Germany could report content under that law. In response to that, we designed into our platforms a way of reporting under that law. We have moderation centres in Germany that were there before. There are more people working in those centres now but, as I said, those centres operate in a global way, and that is part of the general increase in security and safety personnel working within Facebook.

It was not as a direct response to that law. As a direct response to the law, we created a way of reporting, and we took on more lawyers, because what is interesting about netzDG is that it sets quite a tight timeframe for companies to decide whether a piece of content is illegal or not. Sometimes that is very obvious but sometimes it is not. Sometimes it is more of a fringe case of the sort we were just discussing. I know there is a very live debate in Germany about some of the consequences of that law: for example, the risk that it might incentivise people to err on the side of caution and take things down more liberally than they might have done before. We introduced a new reporting system and lawyers. Our content moderation centres in Germany deal with global content and are not a response to that law specifically.

Viscount Colville of Culross: Is your view that the law is encouraging people to take material down which would not be taken down by the legislation?

Rebecca Stimson: All I am aware of is the debate that is happening in Germany. I am not in a position to describe whether that is actually happening. I know that there are a lot of concerns about an unintentional perverse incentive that that law may have encouraged. As you know, very significant fines can be imposed on companies for not removing illegal content quickly, so you can see that where there is what we call an edge case, you would tend to take it down, rather than, as the clock is ticking, spend your time debating whether it is, strictly speaking, illegal. I am aware that it has been quite a controversial piece of law in Germany.

The Chairman: Do you have anything to add?

Katie O'Donovan: I would add that the reviewers make timely decisions about whether the content stays on the platform or is removed. One problem we have heard about from lots of different people over the last couple of years is the scale of the decisions we make, what those decisions are and the timeliness of them. In spring of this year, we started to publish a quarterly transparency report on the content on YouTube that is flagged. We detail it by the category area that it is flagged under and provide information on what happens with the content that has been flagged. That is an iterative process, so each quarter we have been adding more information to that, and we will continue that, based on the areas that people are interested in. To go alongside that, we have also published a user report history for users. If you flag content on YouTube and you want to know what happened to it, you can go on to your report history page, and it will tell you if the content is still live or it has been taken down. Again, that helps people evaluate whether the system is working well at a global level, through our transparency report, or, at a personal level, through the report history.

The Chairman: Let us move on to platform liability. Lord Bishop.

Q180 **The Lord Bishop of Chelmsford:** This follows on from the discussion we have just been having, looking not so much at how you moderate the content when it is there but who is liable and responsible for it being there in the first place. The first question is simple: to what extent should online platforms be liable for the content they host? I am particularly interested because in our previous inquiry, Simon Milner from Facebook gave evidence to us and conceded that Facebook was something in between a publisher and a mere conduit and therefore perhaps there should be some additional liability, particularly in respect of advertising. I understand that you continue to use the word "platform", but what is your understanding of that in terms of liability and, perhaps more generally, responsibility?

Rebecca Stimson: Simon recruited me so obviously everything he says is perfectly accurate.

The Lord Bishop of Chelmsford: But perhaps in this case uncomfortable.

Rebecca Stimson: We have already touched on the statutory responsibilities we have currently under the e-commerce directive and a number of other codes and standards that are applied to us. That tends to apply to illegal content, and, as I said in the previous answer, we broaden that out to a whole range of ways in which we consider ourselves responsible for the content of that platform to ensure that what people are seeing is not harmful, it is not hate speech, bullying and so forth, or containing fake adverts, for example. That is clearly illegal and, again, we have a responsibility under existing law to remove that kind of content. You can take it into fake news. We have done quite a lot on the platform over the last year or so and have removed nearly 500 million fake accounts. We have changed the algorithm that underpins how Facebook works to remove as much fake content as we can. The issues are very big, and there are a huge number of tools in the tool box we can use to deal with them, which reflects the fact that we take a very broad approach to our responsibilities for what is on the platform.

Some people talk about extending the principle of content liability into other areas, and it is worth reflecting on what that would mean if you started to go outside what is illegal and make companies liable for pieces of content that are not illegal but are harmful. I know from our very useful conversations with DCMS, which is thinking about this in the context of the Government's forthcoming White Paper, that, clearly, if you get into that kind of territory, you need to be very clear what the harms are and be very specific about what you are talking about. If you are going to declare something illegal that has not been through both Houses of Parliament but is in some other category, you have a slight risk of confusion and inconsistency there, and you need to be very clear.

The Lord Bishop of Chelmsford: But you can see the problem.

Rebecca Stimson: If you think about the harms you are trying to address and look at the particular successes that we have mentioned in the last couple of answers around how effective self-regulation is in some of those major harms, and the statistics we can all give about how much of this content we are successfully removing, you need to think about extending that principle of liability to a company as well as to the host of the content. It is user-generated content. I think you can see there are some complications there. I am not saying it may not turn out to be a good idea but you have to work from a first-principles basis.

The Lord Bishop of Chelmsford: What do you think should be done to address that issue where you can recognise the harm in the content? It does not seem to me sufficient to say, "We are just the platform".

Rebecca Stimson: The way we operate at the moment, and the way that the Government have been consulting on this, is to look at the policies that we all have at the moment, and their transparency and the reporting on them, to see how well they are being implemented, and we are held to account and scrutiny on that basis. It gets very difficult because all our platforms work in different ways. They have different technologies that underpin them and they serve slightly different purposes. A narrowly drawn prescriptive liabilities law could be quite difficult to implement in practice, and, as we have talked about with netzDG, could have unintended consequences. There should be a broad framework of principles for what we are expected to do, with an emphasis on the transparency, for us to show you what we are doing, and for you to hold us to account.

The Lord Bishop of Chelmsford: That would be helpful.

Rebecca Stimson: We all produce extensive transparency reports and, as you know, that is a big part of the Government's consultation that we are all collaborating on.

The Lord Bishop of Chelmsford: There are some specific issues to do with advertising, but I might let other colleagues come in on that.

Lord Gordon of Strathblane: May I come in on this because it is directly related to the point the Bishop was making? I was going to ask Katie about this. In your evidence, you say in praise of the e-commerce directive that it ensures that those who post material online take responsibility for the content that they produce. The great problem is they do not, frequently, and they leave you with the problem of taking down the offensive material subsequently. Would it not be in your enlightened self-interest if it was not put up in the first place? What steps could we take to help offensive content not appear in the first place, without saying that it is your responsibility?

Katie O'Donovan: I think that is a good synopsis of the conundrum facing us. We want to have an open platform. In the vast majority of cases, it is used in a wholly responsible way. We absolutely see our part in ensuring a responsible framework for the hosting of user-generated content. There has to be some personal responsibility and certainly in YouTube that can be impactful. We have very clear community guidelines and if people breach them, they know their channel can be removed if they do that persistently. That is a serious penalty before you even reach the law. There has been a vast increase in the number of individuals who have been prosecuted for online hate speech or associated crimes in the UK. I think people are beginning to realise that the internet, as Hugh said earlier, is not the Wild West. An element of personal responsibility is key, but it does not need to be this conversation between the e-commerce directive or publisher; there is a balanced situation and a balanced ecosystem that is emerging within that.

Lord Gordon of Strathblane: To go slightly further, do you think it would make your job easier if people were not allowed to post things online unless they had an identifiable traceable address and there was some procedure for seeking redress if something was wrong?

Katie O'Donovan: The question to ask is not necessarily what would make our lives easier. It might make particularly tough questions easier to answer, but we need to think about the detriment to all the law-abiding responsible users who want to upload a video they made in their shed where they have created a model steam engine. The vast majority of content we see on our platform is completely innocuous.

Lord Gordon of Strathblane: And nobody wants to do anything about that. We are talking about the content that you are subsequently asked to take down because it is offensive. Would it not be better if it did not reach you in the first place?

Katie O'Donovan: But how do we stop only that content reaching us and not the positive content?

Lord Gordon of Strathblane: I accept that there are different points of view on anonymity, and anonymity is a benefit in some regimes, but, equally, it means the system could be abused by people who are untraceable.

The Lord Bishop of Chelmsford: To pitch in, you could do some moderation before the content goes up rather than afterwards.

Katie O'Donovan: I have been involved in conversations around anonymity for many years, and I can understand why it sounds like a good solution. Simon gave evidence to a different committee where he said that Facebook requires a real-name policy, and we have certainly seen some issues there. Before I worked at Google, I worked at an organisation called Mumsnet, which is an online forum for women. There is a policy of anonymity on there. People can choose their own names and because they have that anonymity they are able to exchange stories about domestic violence. When I was at Mumsnet, and subsequently, it came under online attack from men’s rights activist organisations which sought to, and did in some cases, illegally share the data of users. It is very difficult to have a system which ends anonymity and does not end the right for people to be able to have really difficult conversations online. The peer-to-peer support that has been enabled for whether it is domestic violence victims or on other issues where people are looking for that element of peer support, is really important. I do not think there is an easy way to end anonymity for the bad guys but keep it for the good guys.

Lord Gordon of Strathblane: Do you think that abuse of the system by the bad guys is a price worth paying to preserve it for the good guys?

Katie O'Donovan: I do not think tolerating abuse is worth it, and we do not tolerate abuse. An open internet for us does not mean a free for all. We abide by the law and everyone who uses our platform has to abide by the law. We also have our own community guidelines that go further and we enforce those and people will be removed from our platform if they break them. It is difficult, complicated and resource intensive but for us it preserves the free internet.

Lord Gordon of Strathblane: Could I ask a further question of Rebecca? A point was made about whether you are a platform or a publisher, and one agrees that it can be a somewhat sterile discussion. Are there objective criteria that would determine where on the spectrum you are, or is it a self-defining matter?

Rebecca Stimson: I can totally understand why this debate is happening. As I said, we have a range of responsibilities, some of them statutory and some of them we assume ourselves for the content that we carry. I can completely understand why Simon—and I do not know if he was in front of this Committee or perhaps a different one—said there is probably a third space in which our responsibilities lie. We do not have editorial boards or teams of journalists, as you have just been talking about in your previous question. We do not moderate content before it goes up. We are clearly not a publisher, but our responsibilities towards the content are a matter of very lively debate around the world.

The Lord Bishop of Chelmsford: I will come in very briefly because it seems to me—and I know I am sounding like a scratched record—that we should be having precisely that debate, and asking whether there is a different category, a different way of defining and describing what you do. From that it might make it that little bit easier, both for you and everybody else, because, frankly, a lot of people get fed up when we hear, "It's nothing to do with us. We are just this wonderful space which people occupy and we can't control it". That is deeply frustrating, which I know you know, but if we put the work in, do you think it might bear fruit? I know we cannot do it now.

Rebecca Stimson: We definitely would not say it is nothing to do with us. I have been quite clear, hopefully, about the responsibilities we feel towards content. I think you could have this debate and it may be fruitful. The approach we are seeing the Government take in the White Paper is that we need to think about what harms we are talking about. That is the focus. Whether you want to label us as something else, a third thing, perhaps that will emerge as the answer to addressing those harms. The approach they are taking is to ask what are we really worried about, where is the underpinning evidence and analysis and what is the best way to address those issues, be that different kinds of regulation, codes of conduct, all the various things we have been discussing this afternoon. It is a slightly second-order issue to work on our definition of what we are, unless it becomes apparent through that process that that is the key to addressing the harms.

The Chairman: May I ask you—because you have implied you might be some sort of third thing—have you defined what that is? Have you discussed internally what that might mean?

Rebecca Stimson: We come at it, as I have just said, from the approach of the harms that we are trying to solve.

The Chairman: No, you indicated and repeated that you are possibly some kind of third thing. Have you had a discussion about what you mean by that?

Rebecca Stimson: We have not had a discussion about defining exactly what that might be because, as I say, we are looking at the debate through a different lens, which is what harms are we trying to tackle and what is the best way to do that.

The Chairman: Should we move on? Baroness Kidron.

Q181 **Baroness Kidron:** I was really struck by something in all of your opening statements, and forgive me if I paraphrase you, but Rebecca said it is really hard to keep abreast of the pace of change, Katie said the ways in which people use technology in their daily lives is changing and Hugh was talking about the question of trust. What struck me about those statements was it was as if you were not engaged or not the motors or not responsible for those things, for that journey.

My question is around design of service, not necessarily about this list of harms we have gone through, but other sorts of ways in which you are pushing the world order. I am randomly grasping this from the air, but one example might be that the vast majority of YouTube videos are watched as recommended by YouTube algorithms. The vast majority are in a loop where you watch one, and it is offered up and you watch the next and the next. Another example is Facebook's decision to have friends of friends on its Messenger service, so, even if you are under 13, your world can extend to friends of friends. I do not want you to hook on to the particular examples. You know from the IWF that we have seen a huge increase in child abuse images, and we talked about that just now, and we have talked about mental health, but we have not talked about what we are seeing in terms of compulsive use and how design of service encourages compulsive use. We have not talked about the fact that spreading data is very difficult. I would like you to talk a little about what you feel your responsibilities are in the design of service that is not about content and those kinds of harms, but pushing the direction of travel, and how you feel about the fact that when you get on the bus, if you get on a bus, every single person on the bus is going to have their phone at their nose. Let us start in a different order with Hugh. He is a bit safer on this particular issue, but please carry on.

Hugh Milward: We are consciously developing technology that will make people redundant. What is our responsibility in that? We know that the pace of change in artificial intelligence, first, is causing people to have fears, and they are right to have fears, and, secondly, they will lose their livelihoods as a result of it. Does that mean we should stop developing it, or does it mean that we should step forward very carefully and design interventions that help to mitigate some of those fears as we go? We have never done this before. The technologists who designed the plough did not think about the impact on those affected by the consequences of that development. This is a new thing that we are bringing closer and closer. We are shrinking the gap between the design of the technology and the design of the mitigating interventions. This is extremely welcome and where we need to go on this. We will not get it right. There will be use cases for technology that we cannot predict now that people will be concerned about. We are taking more, bolder, clearer, more consultative, more collaborative steps in the way we design them now than we have ever taken before.

Rebecca Stimson: I would reflect on a few things. As you know, about a year ago, we made a major change to the algorithms that underpin Facebook to move into more meaningful interactions, to ensure that people were having a better experience online and that there was not so much fake news and clickbait and so on. A large body of evidence suggests that has been very successful. Recently there have been three studies in the US that show that the levels of people engaging with fake news, for example, have dropped by 50% in a year, which is really great stuff. We have also touched on some of the incredible advances in AI and machine learning in addressing some of the worst harms.

Slightly reflecting a previous question, some of those technologies are now so effective at spotting that content, it is almost instantaneous that it is able to take that down, and nobody sees some of it. It is not quite the same as pre-moderation but it is split-second stuff.

We are also all members of lots of global consortiums that are developing technologies, as Katie said in a previous answer, that are useable by smaller platforms. When we get into a conversation about harms, the large platforms are pretty transparent and open and we are held to account. Certainly in our work with the Home Office, they tend to be much more worried about—

Baroness Kidron: To be clear, I am not particularly talking about harms. I am talking about the societal piece.

Rebecca Stimson: The reason I was mentioning them was that we are sharing some of the technology that has resulted from our R&D investment with smaller platforms, to ensure that we are not just hoarding that kind of technology to ourselves. We have a centre—I believe it was established this year—for AI ethics within Facebook, which is looking at these very complicated challenging issues, and we are fully participating in those debates.

Katie O'Donovan: It is a really good question. I agree with the way Hugh described it. The gap between the technology being developed and the mechanisms to help us maximise the potential of that technology, to put it positively, is much smaller. Google, like all big tech companies, has an annual developer conference. It is called Google I/O and is akin to a party conference for tech developers, where you get together and show the brightest and best of the work that you are working on. You have limited time to get stuff in because it is such a high-profile event. Sundar Pichai, our chief executive, spent a significant amount of his presentation talking about the technology that we are developing to help with digital well-being.

You and I have talked about this before. We all find our mobile phones particularly helpful, but we also find that we spend too long on them. The technology we have developed helps people understand what they have spent their time on their phone doing each day. You can set a timer for a particular app, so you might allow yourself to be on email for longer but on social media for less time. It tells you how long you have spent on video platforms. Again, we have adopted some of that technology into YouTube. You can turn off auto play on YouTube. You can find out how long you have been watching YouTube and set a timer. Again, we are developing technology specifically for families and younger people. It is a great question to ask because it is exactly where we should be investing our resources to ensure that technology is a tool that we as people choose how to use and on what terms, and make the most of it that way.

Baroness Kidron: To that point, you mentioned resilience and the amount of money that goes into schools, but one of the things I struggle with is this idea that we create technology that is very problematic for people and try to make them resilient to it rather than we create technology that is really good for people. Even the Time Well Spent movement and the wellness thing is picking up the pieces at the end. I would really appreciate your answers here. There were 17 industrial Factory Acts. There is such a bottom-line issue here and I know you have said you are just little people who are in competition with the others, but look at the share price and your position in the market and think how can we, with your interests, put you in charge of what ethics looks like? How can we not take a more societal view about the development and design of services?

I want to hear from you, but, to put on the record, we have Tristan Harris saying that the technology has hijacked our psychological vulnerabilities. We have John Naughton saying that the future looks pretty bleak because we have a business model of surveillance capitalism. Doteveryone says the design processes and business models of technology need to be strengthened and regulated. I am not going to bore the room, but I have another 12 on this list. I want to ask the question in a slightly more robust way.

Baroness McIntosh of Hudnall: May I add a sentence to amplify what you have just said, in a rather less creative and, you might think, more hostile way? All those interventions you describe, as Baroness Kidron says, are ways of mitigating the problem rather than preventing it, so if somebody switches off, they do, but if they do not switch off, they are still in the world of that particular kind of behaviour. What if all of your interventions were really successful and all the people to whom you were offering the opportunity to mitigate the potential damage that might be done if they go on using those apps, what if that worked, what would that do to your bottom line?

The Chairman: If you could answer this in the round and we will move on.

Baroness McIntosh of Hudnall: I wanted it to be part of the same question.

Rebecca Stimson: I do not think we consider that ethical design has been outsourced to us. I have already mentioned several things that we do within Facebook to ensure ethical design. It depends what you are talking about. It can be anything, from whether our terms of service are clear, accessible and understandable to people, to how we deal with younger users, to algorithms. What we are talking about specifically will depend on the right kind of ethical response. We have a number of ways in the company of doing that, but, as you saw in the Budget yesterday, the Chancellor announced more detail on what the Government's own data ethics centre, I think it is called, is going to be doing. They have announced some really interesting initial work that we look forward to working with them on. We do not feel solely responsible. All the organisations at this table partner with hundreds of organisations around the world, focused on everything from algorithm ethics to child safety and so on. Ideally, we try to address harms before they happen, but where they have happened, we try to stop them happening again. I know you are aware of the many programmes that Facebook runs.

To answer your question, when we changed the algorithm that prioritises what you see on Facebook, our chief executive was very clear that we would take a hit on the bottom line, and we did. We have seen around 50 million fewer hours spent on our platform. We wanted to do that because we wanted it to be a long-term positive and useful product in people's lives; a product that they enjoy and is good for them to contact their friends and family through. It is not in our interests to have it be a terrible, addictive and unpleasant place to spend time, so we have taken a hit on our bottom line and seen less engagement as a result of changes we have made consciously for that reason.

Katie O'Donovan: To build on that, one point I would like to make is that not all screen time can be treated in the same way. People use technology in very different ways. It is good that the Chief Medical Officer is looking into that from a UK point of view to find out what more needs to be done on that. In terms of our bottom line, the way that we operate as a company is that we deliver to people the information that they are looking for. If you look for something on search, you do not want to spend a long time on Google; you want to go through to it. We have built the products because we want them to be used and we want people to be able to manage how long they spend online in a way that works for them.

Baroness Kidron: Katie, I was not talking about screen time, and I absolutely agree with you that not all screen time is equal, but a lot of the design elements have factors and push factors that are not necessarily in the best interests of the person, or at least are somewhat determined by your algorithms that may have stickiness or other things that they want to do.

Katie O'Donovan: That is where we need to clearly define the issue in question and what is needed to be done from a technological point of view.

The Chairman: Who should define? You said "we" need to clearly define.

Katie O'Donovan: The new technology that we announced in the spring to help with digital well-being covered everything from the amount of time you spend on your mobile phone per se, to the amount of time you spend in different apps. Some are enterprise or work apps, some are educational apps, some are multi-purpose apps, where you could be on a social media platform doing something very flippant or you could be on a social media platform contacting your friends and family. For us to understand, we believe that the technology that we announced at our I/O helps users and puts them in control of how much they time they spend online, limits the amount of time they spend online and gives them information about that. They can turn off notifications and bundle notifications. There is a new feature whereby if you put your phone screen down, you will not get any notifications at all. We think all those things are positive innovations in this space, but if they do not go far enough, or if there are further requirements that we would not choose to invest in in technological terms, and society requires of us, it is appropriate for the Government or for your committee to make recommendations in that area.

Baroness Kidron: That is why I am coming back to this idea of outsourcing, because a lot of these things have been responses to various forms of pressure, either in advance of threatened regulation or as a result of regulation. That is really why I am raising the issue. You have all said in answer to the first question, "We are doing rather well and we are doing our best and making these big investments", but is it reasonable to leave you to choose where to make those investments and decide what those boundaries are, or is it not up to society more broadly? I am sorry, Hugh, I interrupted you.

Hugh Milward: The Warnock commission is a very sound model of this. The situation was you had an advancing technology, you had a segment of society that saw the technology almost as its salvation and you had other segments of society that were deeply concerned about the development of this technology. You bring in the country's foremost philosopher, who gathers a group of big minds, and those who are developing the technology, and create an ethical framework by which the development of that technology is guided. That is a very sound set of principles by which we can take forward the development of technology in the UK. I am extremely encouraged by the approach the Government are taking at the moment over the AI Council and certain other aspects. We are finding ways of stepping forward together in the right way, in a way that is not outsourcing those ethical decisions simply to the technology companies.

As we build ethical designs and behaviours into the way we work, we will suffer at the bottom line. That is fine. That suffering at the bottom line will not least be because other cultures that take a different ethical stance or perspective on the way that technology should be used will advance. They will sell into markets and to customers that we will not, and that will mean that we will not be as financially successful. There will be a penalty for that, and we are fine with that.

The Chairman: I think we have bottomed out to quite an interesting issue at the heart of this as to whose responsibility it is to guide you societally, on top of the work you are doing as you develop products, and that is an interesting focus. I thought Mr Milward's analogy was interesting. Sadly, we need to move on. Lord Gordon.

Lord Gordon of Strathblane: To segue from that subject on to another, you are almost arguing for a superregulatory supervisor, which will ensure that self-regulation or co-regulation is working, or point out where it might need to be statutory. Were you arguing for that? I thought you were.

Hugh Milward: It is less about a supervisor and more that, as we take ethical decisions, those decisions cannot be divorced from society. We need to find ways in which we are making sure that they are aligned and consistent and that we are not just bypassing the will of this House and the other.

Lord Gordon of Strathblane: In long-term self-interest, it would be good for everyone if public interest and self-interest were aligned.

Hugh Milward: That would be a marvellous nirvana.

The Chairman: Shall we move on to the final question?

Q182 **Lord Gordon of Strathblane:** Turning to GDPR: what do you think are its strengths and weaknesses? In answering that, all three of you might pay some attention to what Tim Cook of Apple, which I understand has a very different business model from yourselves, said about privacy and everything else on 24 October in Brussels?

Rebecca Stimson: The GDPR established some very important principles, some of them reflected in what we have said today, at the forefront of that being that a user's data is their own and they need to be in control of what happens to it. They need to give clear consent around how it is used and there need to be very clear rules for the use of their data. A harmonising-piece legislation across all 28 member states to drive up standards is an excellent thing.

There are some complications in it, as I said in my first comments. One of your previous witnesses said it was a once-in-a-generation reset of data protection law. I know from my experience as a civil servant looking at it that it is difficult to write anything in this space which is totally future-proof and reflects everything. I remember that there was an interesting debate around rights and expectations of rights. There was a particularly controversial debate around the right to be forgotten and the right to delete. There is a challenge around setting up a right in people's minds and, in practical terms, whether it is possible to delete things once they are out on the internet. It definitely has strengths and weaknesses. It is very early days—it only came into force this year—to judge fully.

Katie O'Donovan: When you ask that question, it is important to ask that question of us, and I will answer it from Google's perspective, but it is a piece of legislation that has impacted almost every organisation in the UK that handles any sort of data. It is worth full and holistic scrutiny. For us, the aims and ambitions of the regulation are exactly as we see them: to give users control over their data and transparency over how it is used. There were a couple of things that we were able to do in advance of the GDPR which very clearly related to the direction the GDPR was going in.

We did some of them because we were able to do them well ahead and before they were instituted in the GDPR, and I can go into a little bit of detail. The information that we provide through My Account, which I mentioned earlier, is really meaningful information, whereby consumers can understand how their information is used by Google and decide what they want to share with us and what they do not. That is really positive and in the spirit of GDPR.

The other thing we have long had as a company—and GDPR now requires other companies to do—is the ability to take out your data. If you have a Google account and you use Gmail, our email provider, you might accrue an enormous number of emails, some photos, your contacts, whatever else, but we wanted to make sure that you could take your data to any other provider, so we have had a system called Takeout, where you can remove your data from Google and take it to another provider. That has been instituted through GDPR and we think it is really positive.

As Rebecca mentioned, having a single set of standards across a large number of people is really helpful. As the UK moves toward Brexit, we hope there is continued data adequacy between the UK and the rest of Europe.

Hugh Milward: In the US, we called for privacy legislation back in 2005, so it is no surprise that we decided very quickly to adopt GDPR as the benchmark for privacy globally for our company. We pretty much treat it as the gold standard in data privacy. What is interesting is that the tools to help manage the privacy settings for our customers that we built on the back of GDPR are now in use world wide. Some 400,000 of those privacy settings, so the second-highest number of users, are in the UK. Interestingly, the highest number is in the US where GDPR does not apply. It is early days and the UK is one of the few European markets that has adopted GDPR in its fullest sense and as early as it has. There are a lot of European countries that have not yet got to the stage that the UK has, irrespective of Brexit. It is still early days but we are very positive.

Lord Gordon of Strathblane: I commend all three of you for being too polite to make any criticism of Tim Cook of Apple, a fellow member of FAANG, because he will be giving evidence next week, and presumably would retaliate. Could we look at how we might make the average user more aware of what you do with the data? Would it be an idea if a little icon lit up on your screen when your data was being collected? Would you object to that?

Katie O'Donovan: Again, it depends what you consider to be data. If you were doing a search on a search engine for Wellington boots, by typing "Wellington boots" your data is being collected. We want to help users to understand what data is and how we use it. We have advertising for My Account across Google, across the search engine at various places where they can do that. We certainly work very hard to communicate how it is used.

Lord Gordon of Strathblane: But you would have no objection to the principle of an icon lighting up when data was being collected?

Katie O'Donovan: I am not a user interface designer but we want users to have more understanding of where their data is being used and how, and have more control over that. That is absolutely how we are building our systems.

Lord Gordon of Strathblane: I see Hugh nodding.

Hugh Milward: The reality is if you take a PC and switch it on, data is being collected. There is data called telemetry. When you plug a new printer into your computer, you expect it to work. It works because there is data being collected about what the printer is and it is being sent to different places, and a small piece of software is installed to make the printer work seamlessly, without the user having to interfere at all. We have had to engineer the operating system so that it is fully compliant with GDPR to allow that kind of system to work, but it works very much in the background. We have built the controls that allow people to determine how that data is collected. The EU-US Privacy Shield ensures that all data is treated completely consistently as between Europe and the US, but we probably need to define what we mean by data collection or use.

The Chairman: You could distinguish between functional data and personal data, could you not?

Hugh Milward: I think you probably could.

Lord Gordon of Strathblane: Another idea that might help the average user is frequently things come up, new terms and conditions, and you are asked, "Do you agree?" A mobile phone is fairly small and most people just press "I agree". Would it not be a good idea, and indeed in your interests, to have your terms and conditions approved or given a kitemark, as it were, by some industry body or co-regulatory body that would simply say, "You are not signing away your house if you sign this"?

Katie O'Donovan: All our terms and conditions have to be compliant with GDPR. It is not an industry body, but it is a legal standard that our terms and conditions have to meet. We have worked hard to make meaningful alternatives available to people too. On YouTube our community guidelines are written very succinctly with cartoon images to illustrate what is meant by those. On Family Link, which is our product for families, and YouTube Kids, we have on-boarding flows that are written in a language and style that is very succinct and easily digestible. We are working to ensure that people understand in a meaningful way how we engage with them.

Baroness Quin: Could the Cambridge Analytica scandal, which was very concerning, happen again, or do you feel that the systems now in place would prevent data being harvested in that way?

Rebecca Stimson: After that happened, there were extensive changes made to the platform as to how apps can and cannot engage with users' data and the control that people have over them. We changed things such as the default settings for interacting with apps and so forth. I would be a bit too brave if I said that something like that could never happen again, but the way that happened has been addressed by all the changes we have made to the platform since. Certainly the evidence we see is that people understand that when they are interacting with social media they are exchanging data and data is being collected. In addition to the kinds of tools that we all have on our platforms, and the availability of our policies, to an awful lot of people it would not matter if they read them anyway; they would not understand. Thus the other half of that coin is about education and support for people to become digitally literate and savvy about what they are seeing. We give an enormous amount of information and transparency about data collection and what we do, but you have to meet the other half of that, to ensure people actually understand the full extent of what they are reading.

Lord Gordon of Strathblane: Most people realise there is a trade-off between you providing very good services, permanently, for nothing, and them providing information about themselves which is useful to you in terms of targeted advertising. What they might be less keen on is you selling that data on and becoming part of a data market.

Rebecca Stimson: We do not sell people's data. That is not how our business model works. If you think about it logically, advertising is what underpins our business, so people’s data is extremely valuable to us, and it would make no sense for us to sell it on. We do not sell people’s data.

Lord Gordon of Strathblane: Could I put a point to Katie? There is a moral difference between looking at what I use Google for, searching for something, whether it is Wellington boots or a holiday in Athens, and targeting advertising at me, which is probably useful to me as well as useful to you financially, and scanning my emails, which you used to do, to see if there was anything. You gave that up. Why did you give it up?

Katie O'Donovan: I do not know why we stopped doing that. I think the intent behind it was the same as showing you adverts for Athens, in that we felt that we may be able to provide some services which were of utility and relevance to the email, but we have stopped doing that.

Lord Gordon of Strathblane: How do you monetise Gmail?

Katie O'Donovan: Some of our products are free to use and do not carry advertising. Some carry advertising on relevant searches. We operate Gmail under the umbrella of Google.

Lord Gordon of Strathblane: If somebody said to you that Google should be split up because it is too large and that Gmail should be a stand-alone service, it would have to close?

Katie O'Donovan: I would not want to hypothesise as to what would happen in those circumstances.

The Chairman: But in itself it would not be a successful business model?

Katie O'Donovan: Again, I have not looked closely under the bonnet of Gmail, but certainly at the moment I believe that it would require a different business model to sustain it.

The Chairman: There is a final point from Baroness Kidron and then we will close.

Baroness Kidron: It has come up a couple of times, the fact you do not sell people’s data, but is it fair to say what you are doing is selling the user to the advertiser? In that exchange, given your share price and the bank accounts of most users, that is quite valuable. The users’ attention is quite valuable to you, and that is why you have designs that encourage use? Would you say that is a fair analysis?

Rebecca Stimson: As I have said, we have re-engineered how Facebook works that has delivered less use, very specifically. When it comes to advertising, we have certainly found when we have done surveys into this that people understand the deal: we have data on them and the advertising means that our service is free for them to use at that point. When you ask them if they would rather have relevant or irrelevant advertising, they say, “If we have to have it to have a free service, we would rather that advertising was relevant”. That is the exchange and trade-off that happens between us gathering people’s data and targeting useful advertising at them, which most people find helpful, rather than the platform being paid for by advertising that is completely irrelevant to them.

Katie O'Donovan: I do not think that is a fair or accurate reflection. Our business model is different from Facebook's in this instance. We run adverts on a small proportion of searches which are relevant to those search terms, where an advertiser will pay when someone clicks on that link. It is not about keeping people on a site or using them as a commodity. It is about relevance and helping people find the information that they need on both a commercial and non-commercial basis.

Hugh Milward: We have a number of different business models that have different monetisation plans around them. Our search engine is very much the same as Katie has mentioned. We have our mail service—originally called Hotmail—and that is self-sufficient in its own right. It is now called Outlook. That is funded by advertising but it is break even in terms of cost.

The Chairman: May I thank our witnesses for their evidence? I am sure you think we have asked quite enough questions, but it may be there are areas that we have not touched on that you would like to comment on. We are going to ask you to offer some clarification in writing on a few points that we discussed earlier and, at the same time, anything you think might be useful to the Committee would be welcome. Do our witnesses have anything they would like to briefly add at this point?

Katie O'Donovan: Thank you very much for inviting us to give evidence.

The Chairman: Thank you for coming and answering our questions. As I say, the clerk of the Committee will be in touch to follow up on a few points.

Facebook UK – supplementary written evidence (IRN0126)

Thank you for the opportunity to follow up on the points raised during the oral evidence session. Apologies for the slight delay in responding. Please find below our response to the questions.

1. How much tax do you pay in the UK as percentage of your turnover?

The UK is home to Facebook's largest engineering base outside the US and we continue to invest heavily here. By the end of 2018 we will employ 2,300 people in the UK and we are doubling our office space in London's King's Cross, with capacity for more than 6,000 workstations by 2022.

Our full accounts for the year ending 31 December 2017 can be found here: https://investor.fb.com/investor-news/press-release-details/2018/facebook-reports-fourth-quarter-and-full-year-2017-results/default.aspx. These accounts reflect the changes we have made over recent years in the way we report tax so that revenue from customers supported by our UK teams is recorded in the UK, and any taxable profit is subject to UK corporation tax. Our UK-specific filing for the year ending December 31 2017 is available here: https://beta.companieshouse.gov.uk/company/06331310/filing-history.

2. Could the establishment of a new horizon-scanning body help to coordinate and empower regulators in the face of an ever-changing digital environment?

As the Committee will be aware, many countries are looking at the question of internet regulation. There are a number of very different models currently in place, and more under consultation. For Facebook, the question is not whether to regulate, but how. We want to work with the UK Government on regulation that achieves our common goal of making the online world safer while supporting a vibrant digital economy.

We are in regular dialogue with the relevant Government departments and a range of other bodies as the Government's Internet Safety White Paper takes shape. The role of the different regulators and how best to co-ordinate them is ultimately a matter for the Government, but I wanted to draw your attention to recent update that Mark Zuckerberg gave on Facebook's content governance and enforcement policies, available here: https://www.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634/. This sets out clearly our thoughts on how we can work towards a thoughtful and collaborative system of co-regulation that focuses on a sensible set of principles and mechanisms which should be flexible enough to account for rapid developments in both our technical abilities and the public's expectations.

3. What lessons have you learnt from the processing of applications for the 'right to be forgotten'? Could this model be used for the processing of complaints about other types of harm?

We facilitate a user's right of erasure in various ways. First of all, users can delete data (content) on a per data-point level themselves via their Activity Log or throughout the Facebook app. In other words they can delete anything they have posted. Users can of course report every piece of content to us if they feel it violates our standards, but where users wish to complain about content based specifically on privacy grounds, they can submit a report using the relevant reporting channel on Facebook. Lastly, users can delete their entire Facebook account if they wish to do so.

The variety of options available for our users to exercise their rights in this area mirrors the variety of ways that we make it easy for users to report other types of negative experience online. We aim to provide people with the tools they need to manage their experience on our platform. Every piece of content on our platform can be reported to us via the user-friendly reporting links which appear beside each piece of content. We continue to use the insights we gain from how people use our platform to improve the ways we handle user reports, and we are also investing in technology to constantly improve our capabilities.

4. Should the law around mergers and acquisitions be changed to create a public interest test (similar to that used in media pluralism cases) in cases of mergers between companies which rely on the use of personal data?

Competition law in the UK is flexible and is well suited to deal with the issues arising in digital industries in the same way as in others. Indeed, the Competition and Markets Authority (CMA) has previously stated that it will consider the likely effects of a merger considering both price and non-price effects which will include impacts on innovation.

Overlaying the CMA's assessment of mergers and acquisitions with a broad public interest test requirement runs the risk of the UK's merger control regime moving away from enforcement grounded in established competition law and economic principles and give rise to business and legal uncertainty. That uncertainty could lead to a chilling effect on investment and is more likely to have the unintended consequence of discouraging innovation (and therefore competition) rather than increasing competition.

5. Some have suggested that social media companies should be required to have their community standards approved by an external body, and for that external body to have the power to ensure that those standards are implemented? What assessment have you made of this proposal?

Since our earliest days Facebook has had Community Standards - the rules that determine what content stays up and what comes down on Facebook. Our goal is to err on the side of giving people a voice while preventing real world harm and ensuring that people feel safe in our community. Our standards are public, you can read them here: http://www.facebook.com/communitystandards.

In April, we went a step further and published the internal guidelines that our teams use to enforce these standards so that these can be scrutinized: https://newsroom.fb.com/news/2018/04/comprehensive-community-standards/. These guidelines are designed to reduce subjectivity and ensure that decisions made by reviewers are as consistent as possible. Finally we also recognize that our polices are only as good as our enforcement, which is why we are publishing quarterly transparency reports so that anyone can see how effective we are at finding and removing content which is against our rules.

The team responsible for setting these policies is global - based in more than 10 offices across six countries to reflect the different cultural norms of our community. Many of them are specialists, with long careers to issues like child safety, hate speech, and terrorism, including as human rights lawyers or criminal prosecutors.

We also already engage with a wide range of external experts and organizations in the design and development of our policies to ensure we understand the different perspectives that exist on issues such as free expression, as well as the impacts of our policies on different communities globally. Every few weeks, the team runs a meeting to discuss potential changes to our policies based on new research or data. For each change the team gets outside input from a range of external parties, often including academics, non-profits, safety organizations, law enforcement, human rights organisations, and other non-government bodies. We've also invited journalists to join this meeting to understand this process. We have now begun publishing minutes of these meetings to increase transparency and accountability. Minutes from the meeting on 13 November can be found here: https://fbnewsroomus.files.wordpress.com/2018/11/content-standards-forum-november-13-2018.pdf.

As we have thought about these content issues, we have increasingly come to believe that Facebook should not make so many important decisions about content on our own. Mark Zuckerberg recently announced that in the next year, we're planning to create a new way for people to appeal content decisions to an independent body, whose decisions would be transparent and binding.[742] The purpose of this body would be to uphold the principle of giving people a voice while also recognizing the reality of keeping people safe.

We believe independence is important for a few reasons. First, it will prevent the concentration of too much decision-making within our teams. Second, it will create accountability and oversight. Third, it will provide assurance that these decisions are made in the best interests of our community and not for commercial reasons.

[742] 'A Blueprint for Content Governance and Enforcement', announcement by Mark Zuckerberg, 15 November 2018: https://www.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634/

Over time, we believe this body will play an important role in our overall governance. Just as our board of directors is accountable to our shareholders, this body would be focused only on our community. Both are important, and we believe will help us serve everyone better over the long term.

As Mark Zuckerberg has said, while creating independent oversight and transparency is necessary, we believe the right regulations will also be an important part of a full system of content governance and enforcement. Services must respect local content laws, and we think everyone would benefit from greater clarity on how governments expect content moderation to work in their countries.

We believe the ideal long term regulatory framework would focus on managing the prevalence of harmful content through proactive enforcement. In reality, there will always be some harmful content, so it's important for society to agree on how to reduce that to a minimum - and where the lines should be drawn between free expression and safety.

A good starting point would be to require internet companies to report the prevalence of harmful content on their services and then work to reduce that prevalence. Once all major services are reporting these metrics, we'll have a better sense as a society of what thresholds we should all work towards. To start moving in this direction, we're working with several governments to establish these regulations.

20 December 2018

Full Fact - written evidence (IRN0071)

Full Fact is the UK's independent factchecking charity. We check the claims of politicians, pressure groups, and the media.

We press for corrections to the record where necessary, and work with government departments and research institutions to improve the quality and communication of information at source.

We have a cross-party board of trustees, and are funded by charitable trusts, individual donors and corporate sponsors. We have received funding from Google and Facebook: details of our funding are available on our website.

Summary

- Freedom of speech is central to any discussion around regulation.

- The Committee has an opportunity to begin a more sophisticated debate about the role of regulation online. This needs to move beyond talk of regulating 'the internet', or even the currently dominant internet companies, to a capabilities and principles based approach that will be more enduring.

- Greater transparency and access to companies' data is needed to understand what is happening on platforms and to evaluate initiatives.

- Online political advertising needs to be regulated and made transparent through open democratic and transparent processes by legislatures, not private companies.

Our submission to the Committee focuses on tackling the problems associated with misinformation on the internet. This is a broad area of issues, which is not new or indeed unique to the online space.

Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

1. The UK should explicitly reject undemocratic or untargeted responses, especially those that undermine freedom of speech or freedom of the press. The government must avoid overstepping the line that protects these freedoms, recognising that historically governments have tended to overreact to emerging communications technologies. We should lead, not follow, our international colleagues.

2. It doesn't make sense to talk about regulation of the internet as a whole. The internet is not a single entity and covers a wide and rapidly-changing set of actors and capabilities.

3. To have a chance at responding successfully to the challenges and opportunities of the internet, we first need to understand the range of capabilities that exist, what power they confer, and then ask what role regulation has to play.

4. We are concerned that without a principles and capabilities based approach, many of the policy conversations in this area risk fighting the last war, and risk being outdated before they are even implemented.

5. The rapidly evolving capability for targeted online political advertising does not have enough oversight. As the Committee's report of April 2018 on Digital Advertising[743] noted, there is not enough transparency in the online advertising market, particularly on how money is being spent.

6. Rules that govern the capability to influence the democratic process by targeting political messages at a micro-level need to be set through open transparent democratic process, not through amendments to online platforms' terms and conditions.

7. Election law must be updated urgently to include the following provisions:

    - The imprint rule requires political advertisers to include the name and headquarters address of the promoter in the advert. This should be extended to online advertising.

    - A database of machine-readable online political adverts should be created, which logs the targeting data and copies of the advert in real time. It must be publicly hosted, not reliant on private companies' policies.

8. The platforms' founders are unlikely to have imagined the scale or range of functions that their companies now consist of, or their influence on society. Nothing in their design prevents a platform from choosing to align itself along particular political lines, or moderating content selectively. Do we therefore take for granted that they are entirely non-partisan, and is this something that should be explicitly stated? The implications of this for freedom of expression warrant a closer look.

What should the legal liability of online platforms be for the content that they host?

9. 'Should the companies be called a platform or publisher' is the most frequently-asked question in discussions about the internet companies' liability for the content on their platforms. Again, the problem with this question is that it does not distinguish between the capabilities these platforms have. We therefore need to take a more nuanced approach to understanding their liability. One product may contain content wholly controlled by users, content wholly controlled by the platform, and content where control is mixed.

[743] https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/116/116.pdf

10. We have prepared a table for the Committee to illustrate what an assessment of platform capabilities might look like (Table 1, annexed). The intention is to demonstrate the breadth of capabilities that the largest platforms provide for their users, but it is by no means a comprehensive list.

How effective, fair and transparent are online platforms in moderating content that they host?

11. Nobody knows.

12. We cannot assess effectiveness or fairness because there is a lack of available data. Platforms must be more transparent and make data available to researchers to independently evaluate moderation practices. Twitter allows some access to its data and Facebook recently announced it would allow access to some researchers regarding specific countries with elections coming up[744]. But these are voluntary efforts that are not applied consistently across platforms.

13. There is a distinction between moderating abusive content, where much of the debate is in this area, and moderating false or misleading content, which is where Full Fact can offer expertise. There is a proportion of inaccurate material than can be cleaned up simply, like spam. But the more vigorous the efforts of online platforms to counter misinformation, the greater the risks to freedom of expression. The focus on fairness as well as effectiveness in the question is vital.

14. Some companies have a clear ethos about the importance of information quality, while for others it is a new area which they are getting to grips with. We know that companies can act fast when they need to. In the weeks leading up to CEO Mark Zuckerberg's appearance before US Congress in April 2018, Facebook moved quickly to announce a raft of measures aimed at tackling information quality and personal privacy[745].

15. Some platforms are also looking to external organisations for help. In 2016 Facebook launched its third-party factchecking scheme, partnering with factcheckers from around the world with the aim of helping to stop misinformation from spreading. This allows Facebook to flag potential false news stories to users and decrease the visibility of pages that repeatedly share false news. The scheme has been set up in several countries including the US, France, Indonesia, the Philippines, Italy and Mexico. It does not yet exist in the UK.

16. When the scheme launched originally, there were concerns about its transparency and effectiveness. More recently, Facebook has been sharing more detail and engaging with factcheckers.

[744] https://newsroom.fb.com/news/2018/04/new-elections-initiative/

[745] https://newsroom.fb.com/

17. The scheme is producing the first large-scale database of articles rated by professional factcheckers for reliability. Mark Zuckerberg has been explicit that he believes part of the future of combating misinformation on Facebook is through artificial intelligence tackling increasingly nuanced problems. This would be possible for Facebook as it holds this database of rated articles which it could use to train machines to spot stories that look similar to the ones in its database. It is vital that such databases and any machine learning that uses this kind of data to affect internet users' behaviour is independently scrutinised to ensure any work is being done in an ethical, fair and responsible way.

What role should users play in establishing and maintaining online community standards for content and behaviour?

18. We shouldn't put too much of the onus of maintaining community standards and responding to the challenges of the internet on users. A report by doteveryone underlines the fact that we should be cautious not to overestimate users' ability to understand the risks associated with the online environment:

> 'There is a major understanding gap around technologies. Only a third of people are aware that data they have not actively chosen to share has been collected. A quarter have no idea how internet companies make their money.'[746]

19. It will continue to get harder for users to make informed choices about what content to trust. For example, it is now easy to use artificial intelligence to combine and superimpose existing images and videos to create fake videos of famous people. This allows the creator to manipulate, for example, real videos of President Obama[747] to say whatever they want. It is difficult even for technical experts to distinguish between the real video and the manipulated video, so there is little hope for the average user.

20. We should focus on trying to help users to make informed decisions, and making those decisions as easy as possible, rather than putting the responsibility for judging content on users.

21. Trusted logos or faces are not enough to prove credibility, because these can also be easily faked, and the speed and scale at which these things can spread make it harder to regulate. Platforms, governments and wider society are going to need to collaborate on new ideas about how to make it easier for users to navigate the content they see.

What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

[746] http://attitudes.doteveryone.org.uk./files/People%20Power%20and%20Technology%20Doteveryone%20Digital%20Attitudes%20Report%202018.pdf

[747] https://www.youtube.com/watch?v=cQ54GDm1eL0

22. Any measures must have freedom of speech and transparency at their core, and this should be explicitly stated. This applies not only to their substance, but how decisions about regulation are made. It may seem pragmatic and practically effective in the short term for the government and private companies to make decisions behind closed doors, but the trade-off is an absence of open transparent democratic process.

23. As we've said above, platforms need to provide more data to academics and factcheckers to allow for independent evaluation and greater transparency of practices. Facebook recently announced a partnership with academics which they say will 'provide independent, credible research about the role of social media in elections, as well as democracy more generally.'[748] Notwithstanding data privacy concerns, we need a frank conversation about access to data across the sector.

24. There is an urgent need for transparency about political advertising practices. Users should be able to see and understand when someone is targeting them with a political advert, and it should be made possible for regulators and civil society to maintain system-wide oversight of what is happening when, who is paying and what the messages say.

25. We welcome what platforms have announced to date. Twitter announced[749] last year that it would be opening a 'transparency centre' that would provide visibility into political and issues-based adverts for users, though no date for delivery has been shared. Google[750] and Facebook[751] have committed to verification for those who place political ads, and Facebook plans to make labelling of adverts clearer.

26. While these efforts are a step in the right direction, certainly from the user perspective, they do not come close to tackling the lack of scrutiny in the sector. That is why updates to election law[752] are needed to hand oversight back to the wider system and protect the integrity of the democratic process. It is not credible for Parliament to wait much longer to bring election law up to date with a dramatically changed world. Important safeguards in election law are ceasing to be effective, while important decisions of principle about how elections should run in the UK are being left to the terms and conditions of private companies.

27. While text based misinformation has been the focus of many projects tackling misinformation so far, images (including memes or infographics), video and audio content are easy manipulated and tend to be harder to track and respond to using technology. First Draft and Farida Vis from the University of Sheffield have been working on a project looking at visual misinformation during the 2017 UK and France elections, drawing on work

[748] https://newsroom.fb.com/news/2018/04/new-elections-initiative/

[749] https://blog.twitter.com/official/en_us/topics/product/2017/New-Transparency-For-Ads-on-Twitter.html

[750] https://support.google.com/adwordspolicy/answer/9011036?hl=en

[751] https://newsroom.fb.com/news/2017/10/improving-enforcement-and-transparency/

[752] See paragraph 7

done in a joint project between Full Fact and First Draft in the UK, with a report forthcoming which we recommend to the Committee.

In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

28. Internet companies should be transparent about the use of their platforms for political purposes, (which can for the avoidance of doubt include the political purposes of commercial or other entities) and ensure that use is accountable, and not using abusive targeting practices. However, we believe this is an area where rule setting may be better done through an open transparent democratic process by legislatures than by the platforms themselves.

29. Platforms should be wary of algorithmic approaches to identifying misinformation. While artificial intelligence technology can help humans spot patterns of behaviour or patterns in content, in the field of misinformation it remains imprecise and should not be relied upon to do the job of human moderators.

30. Broadly speaking, the more specific the problem, the more likely it is that algorithmic approaches will be accurate, and vice versa. Technological solutions to very broad problems are therefore often not realistic or desirable. For example, we believe that trying to develop tech that baldly classifies content as 'true' or 'false' - truth labelling – not only misunderstands the capabilities of the technology, but also the nature of the world we live in.

31. When Mark Zuckerberg testified before US Congress in April, he made it clear that he thought AI would be able to find solutions in next 5-10 years, but that not everything could be automated. This is the right balance. Full Fact's approach has been to identify solvable problems in factchecking and develop technology to solve those specific issues[753].

What is the impact of the dominance of a small number of online platforms in certain online markets?

32. The internet is not - at least not yet - the dominant source of news for most people in the UK, so there is a window of opportunity still for a considered response to emerging technology and its players.

33. While people (especially young people) increasingly consume news online, that shift is not happening as fast as one might be led to believe by coverage of misinformation in the media. TV is still the main source of news for 69% of people in the UK according to Ofcom. This falls to 45% for 16-24 year olds, and rises to 89% for the 65+ age group[754].

[753] https://fullfact.org/automated

[754] https://www.ofcom.org.uk/__data/assets/pdf_file/0016/103570/news-consumption-uk-2016.pdf

34. The current focus on Twitter, Google and Facebook as whole companies is a red herring and does not allow us to see deeply enough into the full capabilities of those and other companies' products. In five years' time, we may be facing different companies, different capabilities, and different products. We urge the Committee to consider principles for regulating now and in future, rather than companies to regulate now.

We'd be very happy to give oral evidence to the Committee if it would be helpful.

May 2018

Full Fact - written evidence (IRN0071)

Annex – Table 1

This document has been produced as an example of an approach for breaking platforms down into functions, and is not designed to be a comprehensive list.

Company		**Alphabet and Google**						**Facebook**				**Twitter**	**Snap**	
Product	Email	Chrome	Gmail	Maps	Play	Google Search	YouTube	Facebook	Whatsapp	FB Messenger	Instagram	Twitter	Snapchat	Others
Worldwide users	3.3bn	>1bn	>1bn	>1bn	>1bn	>1bn	>1bn	2.13bn	1.5bn	1.3bn	800m	330m	180m	
Search														
Provides search results		🟩				🟩	🟩	🟩						
Provides answers to factual questions		🟩				🟩	🟩 Wiki link							
Newsfeeds														
A newsfeed							🟩	🟩			🟩	🟩	🟩	
An algorithmically determined newsfeed							🟩	🟩			🟩	🟩	🟩	
User status														
Systems that do not treat all users equally	🟩		🟩					🟩			🟩	🟩	🟩	
Some users marked as 'verified'								🟩			🟩	🟩	🟩 Discover partners	

Messaging														
Systems for messaging 1-1 between individuals	🟩		🟩					🟩	🟩	🟩	🟩	🟩	🟩	
Systems for messaging 1-many between individuals	🟩		🟩					🟩	🟩	🟩	🟩	🟩	🟩	
Advertising and data														
Displays paid content/ads	🟩	🟩	🟩			🟩	🟩	🟩			🟩	🟩	🟩	
Systems for monitoring users' activity on other internet sites		🟩						🟩		🟩 FB browser				
Systems for monitoring users' activity offline				🟩							By proxy	By proxy	Pilot	
Buying and selling														
Marketplace					🟩			🟩			🟩			
Recommendations														
Makes recommendations					🟩	🟩	🟩	🟩			🟩			

Professor Christian Fuchs, Professor of Media and Communication Studies, University of Westminster – written evidence (IRN0010)

Executive Summary (Key Points)

This submission focused on the following two questions posed by the inquiry:
(#7) In what ways should online platforms be more transparent about their business practices – for example in their use of algorithms?
(#8) What is the impact of the dominance of a small number of online platforms in certain online markets?

- Facebook is built on the idea that gathering and storing as much data about users is good for its profits. The Cambridge Analytica Scandal has shown the problematic implications of the targeted advertising business model and the danger it poses to democracy.
- Research in the projects "Social Networking Sites in the Surveillance Society" and "netCommons: Network Infrastructure as Commons" shows that users have very high concerns about how online platforms use personal data for commercial purposes.
- Given users' high concerns about online corporations' privacy violations and business practices and their strong opposition to online advertising, making online corporations' use of data and algorithms more transparent is not enough. If these processes are made transparent, then users would know more about how online corporations work, but the data collection and processing for the purpose of profit-making and targeted advertising that so many users oppose would simply continue.
- A viable solution to the threats that online corporations' data practices pose for privacy and democracy is to foster alternative, non-profit online platforms. Two options for achieving this goal are public service Internet platforms and platform co-operatives. For achieving a sustainable Internet, policy makers need to advance legislation that enables the creation and financial support of alternative Internet platforms
- Public service Internet platforms would be a counterforce to the monopolies of Facebook, Google & Co. and could open up new spaces and possibilities for content creation, creativity, political online debate, and content distribution beyond the advertising logic of Google and Facebook.
- Introducing an online advertising tax on all ads targeted at users accessing the Internet in the UK would provide a resource base for funding public service and alternative Internet platforms that foster a new online culture.
- Google and Facebook are not just communication and Internet companies; they are the world's largest transnational advertising corporations. Google and Facebook enjoy a duopoly in the field of online advertising: Google is estimated to have controlled 55.2% of global advertising revenue in 2016, and Facebook 12.3%. Google's dominance among search engines and Facebook's among social networks means that there is a trend towards monopolisation. The online advertising duopoly gives Google and Facebook tremendous economic power. In addition, these two corporations have avoided paying taxes.

- Monopolisation is a problem that affects the whole range of digital industries. It is very evident in the realms of online platforms and targeted online advertising dominated by Google and Facebook, but also extends into other areas such as software, telecommunications and Internet service provision. Effective anti-monopolistic policies should involve the legal enablement and financial support of alternative Internet platforms, alternative Internet infrastructure providers, and alternative digital companies that do not follow for-profit logic.

Professor Christian Fuchs, Professor of Media and Communication Studies, University of Westminster – written evidence (IRN0010)

Q1. Background

(§1.1) I am a professor of media and communication studies at the University of Westminster, where I am directing the Communication and Media Research Institute and the Westminster Institute for Advanced Studies. I have over almost twenty years conducted research about how digital media and the Internet impact society in research projects and in activities that have resulted in more than 300 academic publications.

(§1.2) In this submission, I provide evidence relevant by two questions raised by the inquiry:
(#7) In what ways should online platforms be more transparent about their business practices – for example in their use of algorithms?
(#8) What is the impact of the dominance of a small number of online platforms in certain online markets?

Q2. In what ways should online platforms be more transparent about their business practices – for example in their use of algorithms?

(§2.1) Cambridge Analytica paid Global Science Research (GSR) for conducting fake online personality tests on Facebook via the Facebook Developer Platform in order to obtain personal Facebook data of almost 90 million US-users, including likes and friendships. The data was used for targeting political advertisements in elections.

(§2.2) This data breach has caused concerns about social media corporations' business model of targeted advertising and its dangers to democracy. The Cambridge Analytica Scandal was possible because the regulation of data processing for corporate purposes is lax and based on the idea of corporate self-regulation, which invites Facebook, Google, and other digital companies to gather massive amounts of user data and use it for achieving profits. Facebook is built on the idea that gathering and storing as much data about users is good for its profits. Personal data as big data commodity that is used for selling and targeting personalised online advertisements is the underlying business principle of corporate social media, including Facebook, Google and Twitter.

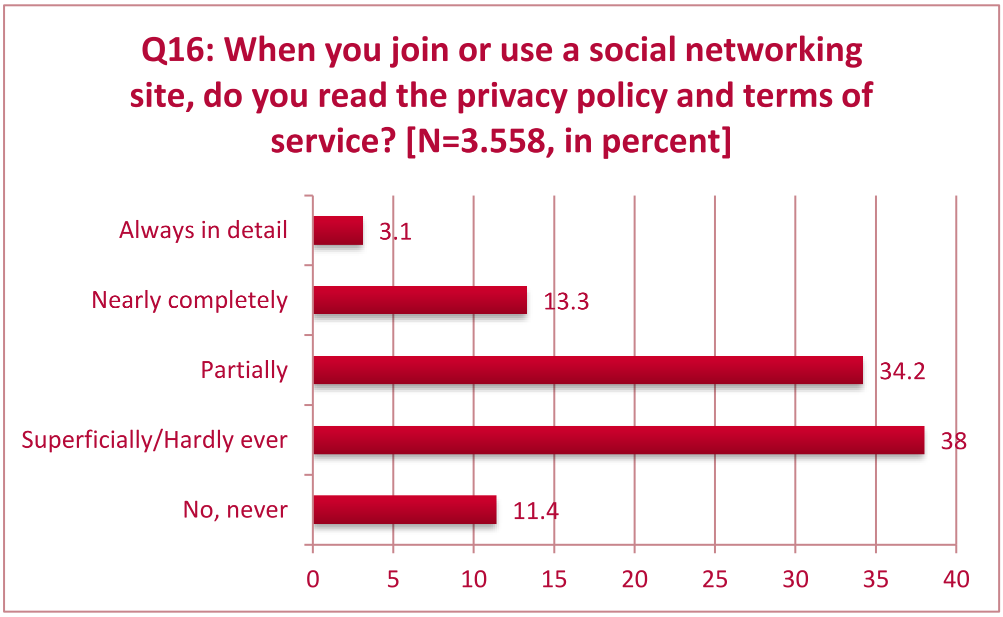
(§2.3) In 2017, Facebook made profits of US$ 15.9 billion almost exclusively from advertising[755]. In the first three months of 2018, Facebook's increased its profits in comparison to 2017 from US$ 3,1 billion (2017) to US$ 5.0 billion (2018)[756]. In the Forbes 2000 ranking of the world's largest corporations, Facebook was in 2017 ranked on position #119 and Alphabet/Google with annual profits of US$ 19.5 billion on position #24. These companies' profitability is based on the digital labour of users who create these businesses' profits through online activities that result in data and meta-data that is used for targeting advertisements (Fuchs 2017b).

[755] https://investor.fb.com/investor-news/press-release-details/2018/Facebook-Reports-Fourth-Quarter-and-Full-Year-2017-Results/default.aspx
[756] https://investor.fb.com/investor-news/press-release-details/2018/Facebook-Reports-First-Quarter-2018-Results/default.aspx

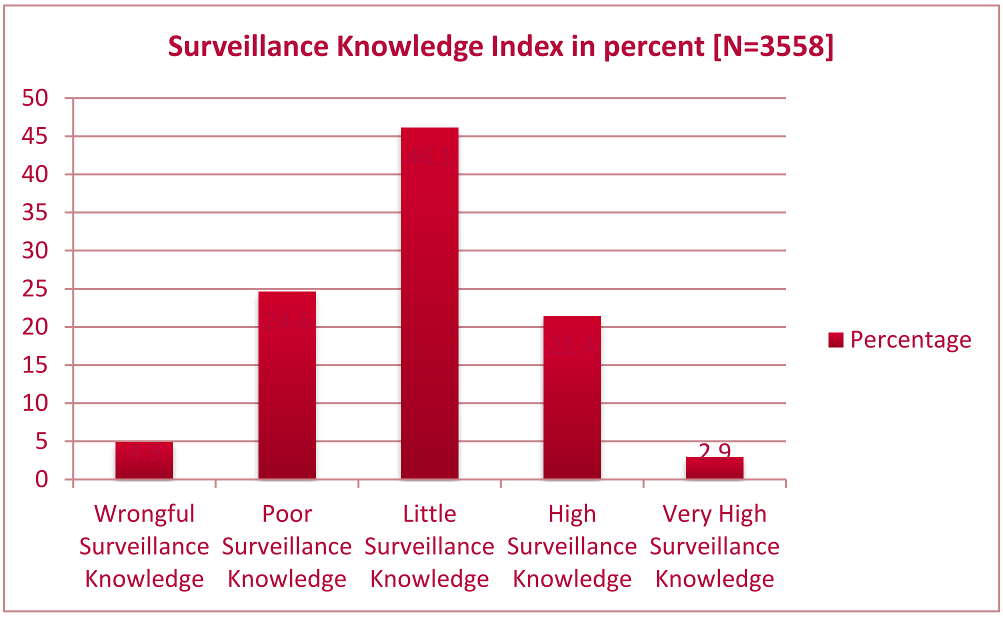
(§2.4) Research that was conducted in projects that I have led has shown that users have little knowledge and large concerns over the commodification of personal data.

(§2.5) In the research project "Social Networking Sites in the Surveillance Society" (SNS3, funded by the Austrian Science Fund, 2010-2014), whose principal investigator I was, we conducted a survey among more than 3,000 social media users (see Kreilinger 2014 for a report summarizing the main survey results):

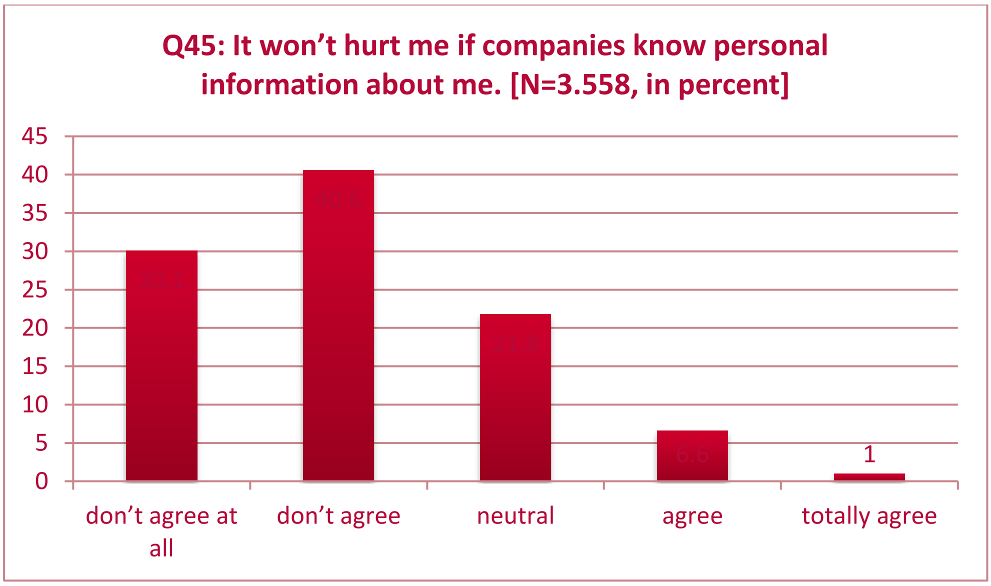
(§2.6) 49.4% of the respondents said that they either never or only superficially read social media platforms' terms of use and privacy policies:



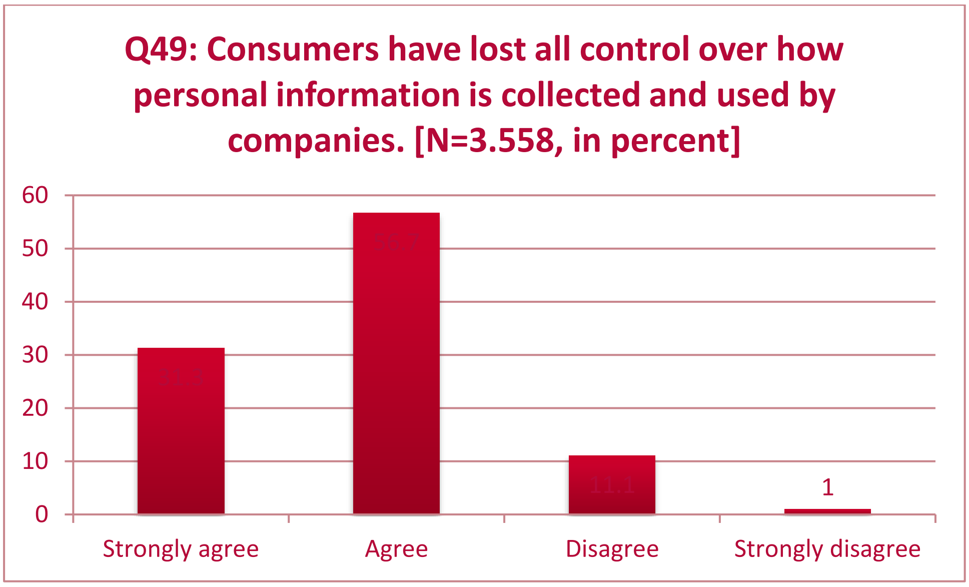
(§2.7) The project measured users knowledge about privacy and surveillance in the context of the Internet and found that 70.7 percent of the respondents had poor or little knowledge about online surveillance:



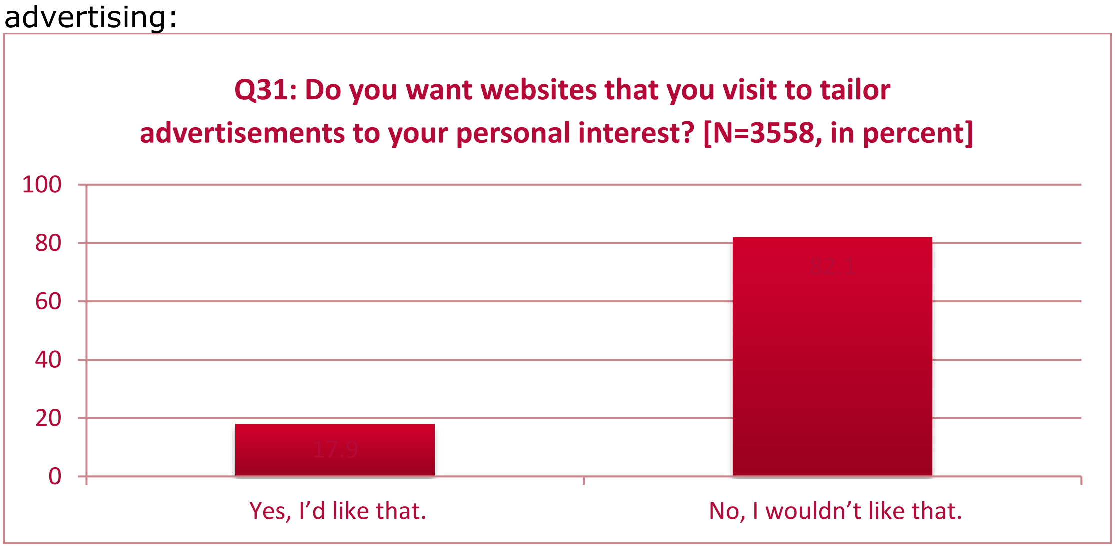
(§2.8) The research also showed that users have large concerns over privacy violations on online platforms. 70.7 percent of the respondents disagreed that companies' control of personal data did not harm them:



(§2.9) 88.0 percent of the respondents agreed or strongly agreed that consumers have lost control over the personal data that companies collect:



(§2.10) 82.1 percent of the respondents said they oppose the use of targeted advertising:



(§2.11) "netCommons: Network Infrastructure as Commons" (http://netcommons.eu) is a three-year EU Horizon 2020 research project (2016-2018), in which the University of Westminster is involved as participating research team under my leadership. The University of Westminster-team (Dr Dimitris Boucas, Dr Maria Michalis, Prof Christian Fuchs) conducted a survey about concerns Internet users have. The netCommons-survey confirmed the result of the SNS3-survey that users are highly concerned about how online corporations use personal data (Boucas, Michalis and Fuchs 2018). 909 out of 1,000 respondents agreed or strongly agreed to the statement "Users do not have control over how personal information is collected and used by online companies". 601 out of 1,000 respondents felt concerned or very concerned in respect to the question "How do you feel about the fact that search engines and social networking sites like Google, YouTube and Facebook use your personal data for profit-making purposes?".

(§2.12) Given users' high concerns about online corporations' privacy violations and business practices and their strong opposition to online advertising, making online corporations' use of data and algorithms more transparent is not enough. If these processes are made transparent, then users would know more about how online corporations work, but the data collection and processing for the purpose of profit-making and targeted advertising that so many users oppose would simply continue. A viable solution to the threats that online corporations' data practices pose for privacy and democracy is to foster alternative, non-profit online platforms. Two options for achieving this goal are public service Internet platforms and platform co-operatives. I have outlined these alternatives in a forthcoming publication (Fuchs 2018):

Public Service Internet

(§2.13) Public service Internet platforms are online platforms run by public service media organisations. They do not have a for-profit imperative, which constitutes a major difference to Google, Facebook, Twitter and other corporate platforms that use targeted advertising. One of the reasons why no alternatives to Californian Internet companies' dominance have been able to establish themselves is that public service media's Internet potential is underdeveloped.

(§2.14) There is a range of conceivable public service Internet platforms whose creation could be financed through an online advertising tax. In the UK, one possibility would be to create a public service emulating YouTube (BBCTube), on which all of the BBC's legally available archive of programmes could be made available to users for reuse with creative commons licences. Users could also upload their own videos to this platform and would have the additional option of remixing and reusing BBC-archive material. Public service broadcasting's educational mandate could thus be realised in the Internet in the form of "digital creativity". This concept could conceivably apply not just to video, but also to audio and radio archive material. There are dozens of public service media institutions in Europe. If all or some of them were to pursue similar projects, then there would be the option of creating a network of these platforms or setting them up as a joint platform, which could establish a popular European public service online media platform able to compete with YouTube, Google and Facebook in terms of popularity and reach. The users would be given ample space to develop their own digital creativity.

(§2.15) Public service Internet platforms would be a counterforce to the monopolies of Facebook, Google & Co. and could open up new spaces and possibilities for content creation, creativity, political online debate, and content distribution beyond the advertising logic of Google and Facebook.

(§2.16) In the UK and Europe, there is a long tradition of public service media. There is no UK or European equivalent of Twitter, YouTube and Facebook because in the UK and Europe there are different media traditions that are to a significant degree based on public service media. Regulatory changes that allow public service broadcasters to offer online formats and social media platforms (such as *Club 2.0* and other formats, see Fuchs 2017c) aimed at advancing political communication and slow media that are advertising-free and adequately funding such activities form a good way of establishing an alternative culture of political communication that weakens fake news culture. Advancing public service Internet platforms is also a step towards overcoming fake news culture.

(§2.17) In the UK, the BBC can play an important role in advancing public service Internet platforms that foster advertising-free political debate that challenges problems such as fake news, fake online attention, a flourishing of hate speech and discrimination online, algorithms that replace human online activities, etc.

Platform Co-Operatives

(§2.18) Platform co-operatives are initiatives that apply the idea of self-managed co-operatives to digital media platforms. The users are empowered to own and control online platforms and to govern these platforms democratically. Platform co-ops are non-profit and commons-based and are run by civil society[757].

(§2.19) One does not have to make a choice between advancing either public service Internet platforms or platform co-ops. Both constitute viable and important alternatives to the corporate Internet.

(§2.20) Advancing alternatives to the dominant logic of online platforms such as Google and Facebook requires funding. Given how critical users are of for-profit online platforms, an alternative logic should therefore be non-profit and advertising-free. Introducing an online advertising tax on all ads targeted at users accessing the Internet in the UK would provide a resource base for funding public service and alternative Internet platforms that foster a new online culture.

(§2.21) Were an online advertising tax to be introduced, there would be the option of using the income thus generated to create public service

[757] See for example: https://platform.coop

Internet platforms, launch a public service Internet offensive, and provide funding to platform co-ops (for example through mechanisms of participatory budgeting).

(§2.21) Is there interest of users in alternative platforms and a new (public service and commons-based) logic of social media and online platforms? In the netCommons-survey, a total of 897 out of 1,000 respondents argued that they would definitely use alternative platforms or that they are interested in such alternatives, when being asked "Would you consider using alternative platforms instead of Facebook, Twitter, YouTube or Google, if this choice would provide better control of your data and privacy?" (Boucas, Michalis and Fuchs 2018).

(§2.22) Creating a sustainable Internet that serves the needs of the users, protects their privacy and interests and overcomes problems such as fake news, the culture of online hate and the lack of digital democracy will not be achieved by fostering transparency of corporate online platforms' unethical practices that users are highly critical of. For achieving a sustainable Internet, policy makers need to advance legislation that enables the creation and financial support of alternative Internet platforms, i.e. both public service Internet platforms and platform co-operatives.

3. What is the impact of the dominance of a small number of online platforms in certain online markets?

(§3.1) In a forthcoming publication that is based on the results of a study of the dominance of Facebook and Google and prospects for taxing online advertising, I have analysed the dangers of monopolies in the online and digital industries (Fuchs 2018):

(§3.2) In economic terms, it is inaccurate to refer to Google and Facebook as communications companies. Rather, they are two of the world's largest advertising businesses. Google and Facebook's profitability is linked to profound changes within the advertising industry. The most significant trend is the marked increase of online advertising and sharp decline in newspaper advertising: newspaper advertising's share of global advertising turnover decreased from 18.3% in 2011 to 12.2% in 2015 (table 1). At the same time, online advertising rose from 20.7% in 2011 to 33.1% in 2015 (table 1).

Year	Total	Newspapers	Magazines	Television	Radio	Cinema	Outdoor advertising	Online	Mobile phones
2005	388,560.1	119,302.7	46,379.5	142,068.0	33,443.4	1,732.3	23,207.9	22,426.3	261.3
2006	415,576.5	121,333.1	48,152.8	150,625.9	34,338.1	1,829.0	24,779.3	34,518.3	336.1
2007	457,407.2	125,263.3	51,493.6	166,606.4	36,238.3	2,184.4	27,856.5	47,764.6	530.7
2008	470,382.8	118,981.9	51,025.0	175,739.6	35,315.2	2,181.7	29,696.7	57,442.6	889.6
2009	409,496.4	95,173.2	38,677.9	159,807.1	30,173.0	2,043.5	25,991.7	57,630.0	1,109.1
2010	453,867.9	96,596.6	39,078.7	185,346.5	32,557.6	2,304.4	27,672.9	70,311.1	1,394.3
2011	493,427.8	98,032.5	39,622.4	201,078.7	33,855.3	2,464.9	29,983.6	88,390.4	3,705.7
2012	502,152.8	90,327.7	35,782.1	207,035.4	34,160.9	2,527.1	30,544.4	101,775.2	7,328.2
2013	511,383.5	83,692.9	33,307.5	209,100.1	34,314.3	2,422.3	30,314.1	118,232.2	14,781.1
2014	524,478.5	75,538.5	29,993.1	212,897.1	34,217.2	2,342.5	30,537.9	138,952.2	27,847.7
2015	499,692.0	62,872.7	24,885.7	194,730.7	31,892.2	2,445.8	28,135.9	154,728.8	47,501.8
Year	**Total**	**Newspapers**	**Magazines**	**Television**	**Radio**	**Cinema**	**Outdoor advertising**	**Online**	**Mobile phones**
2005	100%	30.7	11.9	36.6	8.6	0.4	6.0	5.8	0.1
2006	100%	29.2	11.6	36.2	8.3	0.4	6.0	8.3	0.1
2007	100%	27.4	11.3	36.4	7.9	0.5	6.1	10.4	0.1
2008	100%	25.3	10.8	37.4	7.5	0.5	6.3	12.2	0.2
2009	100%	23.2	9.4	39.0	7.4	0.5	6.3	14.1	0.3
2010	100%	21.3	8.6	40.8	7.2	0.5	6.1	15.5	0.3
2011	100%	19.9	8.0	40.8	6.9	0.5	6.1	17.9	0.8
2012	100%	18.0	7.1	41.2	6.8	0.5	6.1	20.3	1.5
2013	100%	16.4	6.5	40.9	6.7	0.5	5.9	23.1	2.9
2014	100%	14.4	5.7	40.6	6.5	0.4	5.8	26.5	5.3
2015	100%	12.6	5.0	39.0	6.4	0.5	5.6	31.0	9.5

Table 1: Global advertising revenue and various advertising forms' share thereof according to WARC (World Advertising Research Center)-data (data source: https://www.warc.com/), in millions of US dollars and %

(§3.3) If these trends continue, online advertising will soon also at the global level constitute the economically dominant form of advertising. Google and Facebook enjoy a duopoly in the field of online advertising: Google is estimated to have controlled 55.2% of global advertising revenue in 2016, and Facebook

12.3%.[758] Google, which gave itself the new company name Alphabet in 2015, had a turnover of 74.989 billion and a profit of 16.348 billion US dollars in the 2015 financial year[759]. Facebook's 2015 turnover was 17.928 billion US dollars, its profit 3.688 billion US dollars. According to the World Advertising Research Center (WARC), advertising turnover worldwide was 499.692 billion US dollars and global online advertising turnover 154.7288 billion US dollars in 2015 (see table 1). According to these data, Facebook and Google's joint 2015 turnover (91.337 billion US dollars) made up 59.9% of global online advertising turnover and 18.3% of global advertising turnover.

(§3.4) According to the Forbes list of the 2000 largest transnational corporations, the British advertising and public relations company WPP was the 301st largest company in the world and the largest advertising business with a profit of 1.8 billion US dollars in the 2015 financial year.[760] In 2015, however, both Google's and Facebook's profits were larger than WPP's: Google's was nine times higher, Facebook's twice as high. This illustrates the fact that Google and Facebook are the world's most important advertising companies, not traditional advertising corporations. Google and Facebook are not just communication and Internet companies; they are the world's largest transnational advertising corporations.

Tables 2 and 3 show that Google is the world's dominant search engine and Facebook the dominant social network.

Google	70.85%
Bing	11.61%
Baidu	8.14%
Yahoo	7.48%
Ask	0.24%
AOL	0.13%
Excite	0.01%
Other	1.54%

Table 2: Share of the world's online searches carried out on desktop computers in 2016 (data source: NetMarketShare: Market Share Statistics for Internet Technologies, http://www.netmarketshare.com, last accessed 31 December 2016)

[758] https://www.emarketer.com/Article/Google-Still-Dominates-World-Search-Ad-Market/1014258

[759] Data source: Alphabet SEC Filings: Form 10-K (2015), https://abc.xyz/investor/

[760] Data source: http://www.forbes.com/global2000/list/#industry:Advertising, last accessed 8 January 2016.

1	Facebook	1,590
2	WhatsApp	1,000
3	Facebook Messenger	900
4	QQ	853
5	WeChat	697
6	QZone	640
7	Tumblr	555
8	Instagram	400
9	Twitter	320
10	Baidu Tieba	300
11	Skype	300
12	Viber	249
13	Sina Weibo	222
14	LINE	215
15	Snapchat	200
16	Yy	122
17	VKontakte	100
18	Pinterest	100
19	BBM	100
20	LinkedIn	100
21	Telegram	100

Table 3: Number of globally active users (in millions) on social media in April 2016 (data source: SmartInsights, http://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/, last accessed 31 December 2016)

(§3.5) The Herfindahl-Hirschman Index (HHI) is a mathematical, statistical method that can be used to calculate a market's concentration. The following formula is used for this (Noam 2009, 47):

$$HHI_j = \sum_{i=1}^{f} S_{ij}{}^2$$

f = number of companies in industry *j*
S_{ij} = the market share of company *i* in industry *j*
Normalisation to 10,000 (that is, the maximum value is 10,000, standing for the greatest possible concentration: if the index equals 10,000, then there is only one company with a market share of 100%):
HHI < 1,000: low market concentration
1,000 < *HHI* < 1,800: medium market concentration
HHI > 1,800: high market concentration

(§3.6) The Herfindahl-Hirschman Index can be applied to the data represented in Tables 2 and 3 to approximate the degree of concentration in the global search engine and social network markets. To do so, the data need to be ordered by company. If a company owns several platforms, the respective shares of users from each platform need to be added. This is important in the case of Facebook, for example, as WhatsApp, Facebook Messenger and Instagram are all owned by this company. To calculate the degree of social network concentration, we can take the number of global active user profiles on which data are available according to table 5 as our population. The results for search engine concentration and social network concentration are given in tables 4 and 5.

Rank	Company	Search engine(s)	Country	Share (a):	a^2
1	Google	Google	USA	70.85%	5019.7
2	Microsoft	Bing	USA	11.61%	134.8
3	Baidu	Baidu	China	8.14%	66.3
4	Yahoo	Yahoo	USA	7.48%	56.0
5	IAC	Ask, Excite	USA	0.25%	0.1
6	AOL Inc.	AOL	USA	0.13%	0.0
		Other		1.54%	
				HHI:	> 5276.8

Table 4: Calculation of the search engine concentration index

Rank	Company	Number of accounts (in millions)	Platform(s)	Country	Proportion a	a^2
1	Facebook	3890	Facebook, WhatsApp, FB Messenger, Instagram	USA	42.9%	1842.3
2	Tencent	2190	QQ, WeChat, Qzone	China	24.2%	583.9
3	Yahoo!	555	Tumblr	USA	6.1%	37.5
4	Microsoft	400	Skype, LinkedIn	USA	4.4%	19.5
5	Twitter	320	Twitter	USA	3.5%	12.5
6	Baidu	300	Baidu	China	3.3%	11.0
7	Rakuten	249	Viber	Japan	2.7%	7.5
8	Sina	222	Sina Weibo	China	2.4%	6.0
9	Naver	215	LINE	South Korea	2.4%	5.6
10	Snap Inc.	200	Snapchat	USA	2.2%	4.9
11	Yy	122	yy	China	1.3%	1.8
12	Mail.ru Group	100	Vkontakte	Russia	1.1%	1.2
13	Pinterest	100	Pinterest	USA	1.1%	1.2
14	BlackBerry	100	BBM	Canada	1.1%	1.2
15	Telegram Messenger LLP	100	Telegram		1.1%	1.2
	Total:	9,063			**HHI:**	**2536.1**

Table 5: Calculation of the social network concentration index, data source: www.statista.com, accessed on January 2, 2017

(§3.7) It is striking that the fields of search engines and social networks are both dominated by American companies. The Chinese corporation Tencent (QQ, WeChat, Qzone) also plays an important role in the social network field, as it controls three large social networks and thus contributes to the concentration of this global market. Chinese networks usually do not pursue a global strategy. They are instead restricted to services in the Chinese language that target users in China.

(§3.8) In regard to public service media, the analysis of online monopolies shows that there is a very large and hitherto scarcely used potential to create public service Internet platforms to combat the dominance of Google, Facebook and similar Internet businesses in Europe.

(§3.9) In the field of search engines, the Herfindahl-Hirschman Index is larger than 5276.8, and in the field of social networks it is 2536.1. This means that these two economic areas are very strongly concentrated. Google's dominance among search engines and Facebook's among social networks means that there is a trend towards monopolisation. Google and Facebook follow the same economic strategy, namely to use personalised advertising (cf. Fuchs 2017b, chapters 5 and 6). They operate different types of platforms and accordingly offer different information services, but use the same online advertising model, leading to a duopoly in the field of online advertising.

(§3.10) The online advertising duopoly gives Google and Facebook tremendous economic power. In addition, these two corporations have avoided paying taxes, which is in most countries not illegal, but considered immoral by most members of the public. Global corporations amass huge profits and economic power that is further extended by tax avoidance.

(§3.11) In another publication, I have as part of the netCommons-research project analysed information monopolies (Fuchs 2017a):

(§3.12) In 2015, there were 241 information companies among the world's 2,000 largest transnational companies[761]. Together they had combined profits of US$537.3 billion (Forbes, 2015). These profits exceeded the combined GDP of the world's 33 least developed countries (US$474.0 billion) and the combined GDP of the world's 74 smallest economies (US$536.2 billion) (United Nations, 2015 [GDP at market prices in current U.S. dollars]). Table 6 lists the world's 10 most profitable transnational information corporations in 2015.

[761] The following industries were for this purpose classified as information industries: advertising, broadcasting and cable, communications equipment, computer and electronics retail, computer hardware, computer services, computer storage devices, consumer electronics, electronics, Internet retail, printing and publishing, semiconductors, software and programming, and telecommunications.

	Forbes rank	Company	Industry	Profits 2015 (billion US$)
1	40	Vodafone	Telecommunications	77.4
2	12	Apple	Computer hardware	44.5
3	18	Samsung Electronics	Semiconductors	21.9
4	25	Microsoft	Software and programming	20.7
5	20	China Mobile	Telecommunications	17.7
6	39	Google	Computer services	13.7
7	44	IBM	Computer services	12.0
8	67	Intel	Semiconductors	11.7
9	88	Oracle	Software and programming	10.8
10	22	Verizon	Telecommunications	9.6
				Total: 240.0

Table 6: The World's Most Profitable Transnational Information Corporations, 2015. Data source: Forbes (2015)

(§3.13) The combined profits of the world's 10 largest transnational information corporations (US$240.0 billion) are larger than the combined GDP of the world's 16 least developed countries (US$229.2 billion) and larger than the combined GDP of the world's 54 smallest economies (US$234.2 billion; United Nations, 2015 Data [GDP at market prices in current U.S. dollars]). Vodafone was, in 2015, the world's most profitable transnational information corporation. Its profits amounted to US$77.4 billion. Vodafone's profits were larger than the individual economic performance of 114 of the world's countries (World Bank Data, GDP at market prices in current U.S. dollars for 2015), including populous countries such as Ethiopia (100 million inhabitants), the Democratic Republic of Congo (75 million), Tanzania (52 million), Kenya (45 million), and Uganda (38 million) (United Nations 2015).

(§3.14) These data show the power of transnational information corporations. They are very profitable companies. Their individual economic power is often larger than that of entire countries. Their profitability is often enhanced by tax avoidance.

(§3.15) Monopolisation is a problem that affects the whole range of digital industries. It is very evident in the realms of online platforms and targeted online advertising dominated by Google and Facebook, but also extends into other areas such as software, telecommunications and Internet service provision. Effective anti-monopolistic policies should involve the legal enablement and financial support of alternative Internet platforms, alternative Internet infrastructure providers, and alternative digital companies that do not follow for-profit logic.

References

Boucas, Dimitris, Maria Michalis and Christian Fuchs. 2018. *D5.4: Alternative Internet Survey Analysis and Interpretation of Data. netCommons Deliverable No. D5.4*. Forthcoming publication on http://netcommons.eu (to be published in June 2018).

Forbes. 2015. *Forbes 2000 List of the World's Biggest Public Companies, 2015 List*. Retrieved from https://www.forbes.com/global2000/

Fuchs, Christian. 2018. *The Online Advertising Tax as the Foundation of a Public Service Internet*. London: University of Westminster Press. Forthcoming open access book on https://www.uwestminsterpress.co.uk/ (to be published in June 2018).

Fuchs, Christian. 2017a. Information Technology and Sustainability in the Information Society. *International Journal of Communication* 11: 2431-2461.

Fuchs, Christian. 2017b. *Social Media: A Critical Introduction*. London: Sage. Second edition.

Fuchs, Christian. 2017c. Towards the Public Service Internet as Alternative to the Commercial Internet. In *ORF Texte No. 20 – Öffentlich-Rechtliche Qualität im Diskurs*, 43-50. Vienna: ORF. http://fuchs.uti.at/wp-content/ORFTexte.pdf

Kreilinger, Verena. 2014. *Research Design & Data Analysis, Presentation, and Interpretation: Part Two. Social Networking Sites in the Surveillance Society (SNS3)* Research Project Report #14. ISSN 2219-603. http://sns3.uti.at/wp-content/uploads/2010/09/The%20Internet%20Surveillance%20Research%20Paper%20Series%2014%20Verena%20Kreilinger.pdf

Noam, Eli. 2009. *Media Ownership and Concentration in America*. Oxford: Oxford University Press.

United Nations. 2015. *United Nations Human Development Report*. Washington, DC: UNDP.

3 May 2018

The Global Network Initiative (GNI) - written evidence (IRN0046)

The Global Network Initiative (GNI) respectfully submits the following information in response to the Committee's call for evidence regarding its inquiry on "The Internet: to regulate or not to regulate?" GNI is a multistakeholder initiative that brings together Information Communications and Technology (ICT) companies, civil society organizations, investors, and academics to forge a common approach to protecting and advancing freedom of expression and privacy online.

1) Introduction

1.1 GNI encourages governments around the world to carefully consider how they can help ensure that the Internet remains both an open and interoperable global network, as well as a secure and safe space for users with diverse demographics, backgrounds, and views. Given the speed with which associated technologies and social practices evolve, we recognize that the Internet may occasionally present novel and unique challenges that may require, equally, novel and unique policy responses. However, those responses will be more effective and less likely to result in unintended consequences if they are carefully considered, evidence-based and developed in consultation with experts and stakeholders. For those reasons, we welcome this Committee's transparent and participatory approach.

1.2 As the Committee considers "regulation" of the Internet, it is important to underscore that regulation can include a wide spectrum of arrangements between relevant actors, including voluntary commitments by companies on one end, and binding laws with government enforcement on the other. In between these poles, lie a range of possible arrangements that may exhibit various degrees of flexibility, transparency, and accountability.

1.3 Multistakeholder initiatives like the GNI, which are based on voluntary commitments by companies, informed by and assessed in collaboration with other stakeholders, represent one form of arrangement that can be considered to address various challenges related to the Internet.

1.4 In order to further inform the Committee about this particular example of how multistakeholder initiatives can work, GNI has provided details in this submission regarding its structure and activities. However, we want to be clear that GNI's focus is specifically on situations where companies face government restrictions that can negatively impact the rights of their users. We are not suggesting that GNI should be used to address other related or distinct concerns that may be considered by this Committee during its deliberations.

2) GNI's Governance

2.1 GNI's launch in 2008 was a result of proactive and collective efforts by ICT companies, human rights and press freedom organizations, academics, and investors to address increasing demands by governments on ICT companies to censor and/or hand over user data. GNI has developed a set of Principles (the Principles) and Implementation Guidelines (the Guidelines) based on international human rights laws and standards, which guide responsible company action when facing restrictions from governments around the world that could impact the freedom of expression and privacy rights of users, and to which all GNI members commit. More than 1.5 billion people in over 120 countries in Africa, North, Central and South America, Europe, the Middle East and the Asia-Pacific are affected by the standards and user rights protections outlined by GNI principles.

2.2 To ensure accountability, GNI assesses member company compliance with the GNI Principles and Implementation Guidelines. The assessment process seeks to determine whether GNI member companies are making good faith efforts to implement the Principles and demonstrating improvement over time.

2.3 On the basis of the trust built among members through assessment, GNI also fosters internal shared learning. Harnessing the collective intellectual and practical experience and capability of our diverse membership enables GNI to bring unparalleled resources to bear upon new challenges at the intersection of free expression, privacy, and the ICT sector. In addition to structuring and facilitating internal discussion and information exchange, we also proactively engage external stakeholders through our annual learning forum and other topic-specific learning events.

2.4 Lastly, GNI actively engages in relevant policy discussions to promote rule of law and the development of laws, policies and practices that promote and protect freedom of expression and privacy. GNI's policy work includes support for and amplification of the work that our members conduct in their individual capacity, as well as coordinated and collective engagement through GNI.

2.5 GNI is a not-for-profit corporation registered in the United States, with a small staff located in both Europe and the U.S. GNI is governed by a board composed of representatives of our four constituencies (civil society, ICT companies, academics, and investors), and our board is chaired by Independent Board Chair Mark Howard Stephens, CBE.

3) The GNI Principles on Free Expression and Privacy

a. Multistakeholder Collaboration

3.1 GNI facilitates a collaborative approach to problem solving and explores new ways in which the collective learning from multiple stakeholders can be used to advance freedom of expression and privacy. The members commit to 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.

b. Responsible Company Decision Making

3.2 GNI member companies commit to responsible company decision making by aligning their policies, procedures, and processes with the Principles. In addition to ensuring that key decision makers are informed of the Principles, GNI requires companies to proactively identify circumstances where freedom of expression and privacy may be jeopardized or advanced and integrate the Principles into their decision making in these circumstances.

3.3 GNI expects participating companies to implement the Principles when they have operational control. When they do not have operational control, we ask participating companies to use best efforts to ensure that business partners, investments, suppliers, distributors and other relevant related parties follow these Principles. In implementing the Principles, GNI expects companies to prioritize the safety and liberty of company personnel who may be placed at risk.

c. Freedom of Expression

3.4 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.

3.5 GNI asks participating companies to respect and work to 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 commit to protect the free expression rights of users when confronted with government demands that are inconsistent with internationally recognized laws and standards.

d. Privacy

3.6 GNI believes 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.

3.7 Under GNI Principles, participating companies are asked to employ protections with respect to personal information in all countries where they operate in order to protect the privacy rights of users. In addition, participating companies commit to respect and work to protect the privacy rights of users when confronted with government demands, laws or regulations that compromise privacy in a manner inconsistent with internationally recognized principles and standards.

e. Governance, Accountability and Transparency

3.8 A governance structure that supports the purpose of the Principles is crucial in ensuring companies' sustainable commitment to the Principles. Participating companies must be held accountable for their role in the advancement and implementation of these Principles. GNI requires participating companies to adhere to a collectively determined governance structure, with defined roles and responsibilities for participants. Companies are further held accountable through a system of (a) transparency with the public and (b) independent assessment and evaluation of the implementation of the Principles.

4) The GNI Implementation Guidelines

4.1 GNI Guidelines provide a more detailed roadmap to ICT companies on how to put the Principles into practice, and also provide the framework for assessment and collaboration among company, NGO, investor and academic members. The Guidelines are available on our website at: https://globalnetworkinitiative.org/implementation-guidelines/.

5) Company Assessment

5.1 Companies participating in GNI are independently assessed every two years on their progress in implementing the GNI Principles. The purpose of the assessment is to enable the GNI Board to determine whether each member company is "making good faith efforts to implement the GNI Principles with improvement over time." The assessment is made up of a review of relevant internal systems, policies and procedures for implementing the Principles and an examination of specific cases or examples that show how the company is implementing them in practice.

5.2 After self-reporting from the companies to GNI after the first year of membership, an independent assessment is conducted of each company member beginning in their second year and then repeated every two years. This assessment is conducted by independent, GNI-accredited assessors and includes both a review of company systems and processes, as well as the review of specific, timely, and topical case studies.

5.3 The GNI assessment process is confidential. This allows GNI's multistakeholder Board to review and discuss in detail sensitive case studies of government requests from countries around the world. It also allows the GNI to review the evolution of the internal systems, processes, and policies our member companies use to protect the privacy and free expression rights of their users.

5.4 It is the role of the GNI Board to review the company assessments and to conclude whether the GNI member company is making good faith efforts to implement the Principles with improvement over time. The GNI's evaluation of compliance by participating companies will be based on an assessment of the totality of a company's record during the assessment phase to put into operation the Principles and the Implementation Guidelines.

11 May 2018

Global Partners Digital – written evidence (IRN0099)

1. Global Partners Digital (GPD) is pleased to respond to the Select Committee on Communications' call for evidence as part of its inquiry, "The Internet: To Regulate or Not To Regulate?".

2. GPD is a social purpose company dedicated to fostering a digital environment underpinned by human rights and democratic values. We work with a range of stakeholders around the world – including governments, businesses and civil society organisations – in pursuit of two core aims: to empower a wider diversity of voices to engage in internet-related decision-making processes; and to make these processes more open, transparent and inclusive.

3. We respond, in this submission, to questions 1, 2, 3, 5, 6 and 7 in the call for evidence. While the first of these questions relates refers to regulation of the internet generally (a point we address in our response to that question), the rest relate solely to online platforms and, specifically, issues of intermediary liability (question 2), content moderation (questions 3 and 5), data protection (question 6) and transparency (question 7). We hope that, as a result of our experience and ongoing work on the issues raised, we are able to provide useful insight and perspectives.

Question 1: Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

4. Before answering this question, we note that while it asks whether 'the internet' requires specific regulation, the focus of the call for the evidence and the questions asked is on online platforms. While online platforms are undoubtedly a significant part of the internet for many individuals, they represent just one part of it. In its broadest sense, 'the internet' comprises a number of layers including physical infrastructure, networks, protocols, coding and the applications which sit on top of those lower layers. Platforms which allow users to generate, search for and share content represent just one part of that application layer.

5. What the Committee refers to as 'regulation of the internet' appears to us to be, in fact, 'regulation of online platforms'. As a preliminary point, we would urge the Committee to make clear in its final report the precise scope of the inquiry to avoid misunderstanding. Our answer to this and the remaining questions, rests on the understanding that the focus is on online platforms, rather than the internet in its entirety.

6. To respond directly to the question, we do not believe that there is a need to introduce specific regulation for the internet. We do not believe specific regulation would be desirable or an effective means of addressing the challenges which the Committee has highlighted, such as fake news, hate speech and abuse, 'extremist' content, or the questionable collection and use of personal data. Those challenges are not unique to the internet, but predate them. While we recognise that the internet has created new ways by which these challenges present themselves, not least due to its global nature, it is ultimately only the *means* by which they are manifested, not the challenge itself. As such, we believe that these and other challenges should be addressed through existing frameworks, adapted as necessary to meet the technical and other differences specific to the internet.[762] In our responses to questions 2, 3, 5, 6 and 7, we set out how online platforms - supported by government action - can better address these challenges.

Question 2: What should the legal liability of online platforms be for the content that they host?

7. From a human rights perspective, the role that online platforms play in facilitating enjoyment of that right to freedom of expression is difficult to overstate. The statistics speak for themselves: Facebook, the world's largest social media platform, has more than 2 billion active users each month.[763] As of July 2015, more than 400 hours of video were being uploaded onto YouTube every minute.[764] Every day, hundreds of millions of tweets are sent on Twitter.[765] Online platforms allow millions of people - in the United Kingdom and worldwide - to communicate, seek and share information, and express themselves.

8. The impact that online platforms have had upon freedom of expression has been recognised at the highest levels. In 2016, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression noted that:

> "*The contemporary exercise of freedom of opinion and expression owes much of its strength to private industry, which wields enormous power over digital space, acting as a gateway for information and an intermediary for expression.*"[766]

9. In considering the question, therefore, of what legal liability should be attached to online platforms for content they host, it is important to recall that states have an obligation under Article 19 of the International Covenant on Civil and Political Rights (ICCPR) to respect, protect and fulfil the right to freedom of

[762] We strongly agree with the statement of Dr Victoria Nash in giving evidence to the Select Committee on 24 April 2018 that "[a]s for whether we need a new regulatory framework for the internet and whether that is desirable or possible (...), we do not need a new regulatory framework at this point. What we need is to use the frameworks that we have more effectively."

[763] Titcomb, J., "Facebook now has 2 billion users, Mark Zuckerberg announces", *The Telegraph*, 27 June 2017.

[764] Bergman, S., "We Spend A Billion Hours A Day on YouTube, More Than Netflix And Facebook Video Combined", *Forbes*, 28 February 2017.

[765] Twitter, "How Policy Changes Work", *twitter.com*, 20 October 2017, available at: https://blog.twitter.com/official/en_us/topics/company/2017/HowPolicyChangesWork.html.

[766] United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc. A/HRC/32/38, 11 May 2016, Para 2.

expression.[767] Given the important role that online platforms play in facilitating the right to freedom of expression, governments, including the UK government, should ensure that any legislation which is of specific application to online platforms does not restrict freedom of expression explicitly or in its effects. Inappropriate legislation which attaches liability to online platforms for content which is available on them, can lead to a 'chilling effect' in which platforms either become reluctant to host or otherwise make available content, or are overly zealous in removing content which might be harmful.[768] It can also result in online platforms being forced to make decisions about the legality of content which they are ill-equipped to make, a problem exacerbated due to the minimal transparency that exists regarding online platforms' decisionmaking, and the absence of due process, safeguards for affected users, and oversight.

10. As such, developing any liability regime requires careful consideration. There are, at present, a range of liability regimes across the world which fall within three broad categories:

Liability regime	Summary	Example
Strict liability	Platforms are held liable for unlawful or harmful content made available by users on their platforms, even if they are not aware of the content.	Thailand (Section 15 of the Computer Crimes Act 2007)
Conditional liability / 'safe harbour'	Platforms are not held liable for unlawful or harmful content made available by users on their platforms *provided* they do not have any knowledge of the content or, if they do have knowledge, have acted expeditiously to remove that content.	European Union (Article 14 of the E-Commerce Directive)
Broad immunity	Platforms are, as a general rule, not held liable for unlawful or harmful content made available on their platforms, even if they are aware of the content. Some limited exceptions may exist, such as for certain specified crimes or intellectual property.	USA (Section 230 of the Communications Decency Act)

11. 'Strict liability' regimes are the most likely to result in overly broad restrictions of freedom of expression, as they require the platform proactively to monitor and remove content, even without notification of its potential illegality. However, even 'safe harbour' or 'conditional liability' regimes can be problematic where the conditions under which liability will be held are such that they require a platform to make determinations about the lawfulness of content, to remove content within short time limits or impose high sanctions for a failure to take

[767] The UK ratified the ICCPR in 1976. Along with all other member states of the Council of Europe, it also has similar obligations under Article 10 of the European Convention on Human Rights.

[768] See above, note 5, Para 43.

down content. In such circumstances, there is a clear incentive on platforms to 'play it safe' and remove ambiguous content so as to avoid liability and potential fines or other sanctions.

12. One example of such a liability regime is the Network Enforcement Act (NetzDG) in Germany. The NetzDG requires platforms with more than two million subscribers to remove "manifestly unlawful" content within 24 hours with fines of up to €50 million for non-compliance. The law has been criticised for incentivising platforms to taking down content unnecessarily,[769] and, since coming into force on 1 January 2018, has resulted in questionable removal of content such as satirical tweets on Twitter.[770]

13. While we do not consider that intermediaries should *never* be liable for content which is made available on their platforms, we consider that there ought to be sufficient limitations and safeguards in place when it comes to attaching liability to ensure that risks to freedom of expression through incentives to remove content are effectively mitigated. We believe that such a regime is feasible through compliance with the following principles, drawn from existing international human rights standards and documents of best practice, notably the Manila Principles on Intermediary Liability[771] and Council of Europe Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries.[772]

    - First, the development of any legislation which attaches liability to platforms should be open, inclusive and transparent. The development process should include consultation with all relevant stakeholders and governments should consider undertaking a human rights impact assessment to understand the impact that the legislation may have on human rights.

    - Second, the legislation itself should be consistent with the principle of legal certainty. This means that it should be accessible, and sufficiently clear and precise for platforms, users and other interested groups to be able to regulate their conduct in accordance with the law.

    - Third, the legislation should not directly or indirectly impose a general obligation on platforms to monitor third party content where they do nothing more than host that content, or transmit or store it, whether by automated means or not. Further, the legislation should not attach strict liability to a

[769] See, for example, the letter from David Kaye, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, to the government of Germany on 1 June 2017, available at: http://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf.

[770] Oltermann, P., "Tough new German law puts tech firms and free speech in spotlight", *The Guardian*, 5 January 2018.

[771] The Manila Principles on Intermediary Liability, available at: https://www.manilaprinciples.org, were developed by a group of civil society organisations in 2015, and provide a set of best practices guidelines for in relation to intermediary liability. David Kaye, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, has praised them as "a sound set of guidelines for States and international and regional mechanisms to protect expression online" (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*, UN Doc. A/HRC/29/32, 22 May 2015, Para 54).

[772] Council of Europe Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, available at: https://rm.coe.int/1680790e14.

platform for hosting unlawful content as this would, de facto, require such monitoring.

- Fourth, the legislation should not directly or indirectly impose liability on platforms for third party content where they do nothing more than host that content, or transmit or store it, whether by automated means or not, and have no actual knowledge of specific content thereby hosted, transmitted or stored. Indeed, the legislation should explicitly exempt platforms from liability in such circumstances.

- Fifth, the legislation should not attach liability to platforms for failing to restrict lawful content.

- Sixth, the legislation should not provide any incentives to remove content which may be lawful, such as via unrealistic timeframes for compliance, or the imposition of disproportionate sanctions for non-compliance.

Question 3: How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

Question 5: What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

14. We have chosen to answer questions 3 and 5 together as they relate to the same issue, namely how online platforms should respect the right to freedom of expression, including through their content moderation policies and processes.

15. As noted above in paragraphs 7 and 8, it is now recognised that online platforms play a key role in facilitating the right to freedom of expression. While, as businesses, online platforms do not have obligations under international human rights law in the same way that states do, the development and adoption of the UN Guiding Principles on Business and Human Rights (the Guiding Principles) in 2011 has, for the first time, established a clear framework for the role of businesses when it comes to human rights. The Guiding Principles are clear that all businesses have a responsibility (rather than a legal obligation) to respect human rights, to avoid causing or contributing to adverse human rights impacts through their own activities, and to address such impacts when they occur.[773]

16. As well as this framework, the role of platforms in relation to content has changed in recent years in a way which further brings their responsibilities into

[773] See, in particular, Principle 11 which requires business enterprises to respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved. Principle 13 sets out the responsibility to respect human rights as including a requirement that business enterprises avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur. Principle 14 makes clear that the responsibility of business enterprises to respect human rights applies to all enterprises regardless of their size, sector, operational context, ownership and structure. Principle 15 requires businesses to enable the remediation of any adverse human rights impacts they cause or to which they contribute.

sharper focus. Traditionally, a distinction could be made between platforms which merely hosted content and made no editorial decisions about that content, and publishers which did make such decisions. This distinction is crucial since many legal regimes across the world – such as Article 14 of the European Union's Directive on electronic commerce, noted above – exclude liability for content merely hosted by a platform or other company unless they are notified, or otherwise become aware, of content being hosted which is unlawful.[774] As such, platforms which merely host content have no proactive duty to monitor that content in those jurisdictions.

17. But online platforms are no longer entirely neutral in hosting and making available content online. Many use algorithms which determine the manner and order in which content is available, make recommendations to users to access certain content, and promote targeted advertising. Many also proactively monitor content to make decisions about its compliance with their Terms of Service. As such, they are no longer passive, neutral hosts of content generated by their users. And the greater their involvement in making decisions about the content we see, the greater their impact upon users' right to freedom of expression and thus the greater their obligations under the Guiding Principles.

18. Despite this, concerns persist that online platforms are failing to respect their users' right to freedom of expression. Between 2014 and 2016, the Center for Technology and Society of Fundação Getulio Vargas Rio de Janeiro Law School analysed the Terms of Service of 50 major online platforms in order to assess how they dealt with human rights, including the right to freedom of expression.[775] Their conclusion was clear:

> *Online platforms offer few guarantees in their policies on preserving the right to freedom of expression. There is a lack of clear and specific information in the Terms of Service on which content is allowed or not in the platform. There is also little commitment to offering users justification, notice and the right to be heard when content is removed by the platforms' own initiative or after notification from third parties.*[776]

19. In 2017, the Ranking Digital Rights Corporate Accountability Index reviewed 22 major internet, mobile, and telecommunications companies and found that they published little information on their policies which affected users' right to freedom of expression, when they removed users' content or suspended their accounts, or what grievance and remedial mechanisms existed for users to challenge decisions to remove content or suspend accounts.[777]

[774] Article 14 of the Directive on electronic commerce (Directive 2000/31/EC), for example, provides that service providers should not be held liable for content hosted unless (a) they have "actual knowledge" of its illegal nature or (b) upon obtaining such actual knowledge, they fail to act expeditiously to remove or to disable access to the content.

[775] Venturini, J. and others, "Terms of Service and Human Rights: an Analysis of Online Platform Contracts", 2016, Editora Revan.

[776] *Ibid*., p. 96.

[777] Ranking Digital Rights, Corporate Accountability Index 2017: Key Findings, available at: https://rankingdigitalrights.org/index2017/findings/keyfindings/.

20. As well as this lack of transparency, there have been a number of high profile examples of inappropriate content removals. In 2017, YouTube deleted a number of videos containing evidence of atrocities in Syria.[778] On Twitter, the accounts of verified news channels and users who have complained of harassment have been suspended.[779] In 2016, Facebook deleted posts of a famous photograph of a napalm victim in the Vietnam War.[780] While, in some instances, platforms have sought to remedy the situation, it has often only been following public pressure. The scale of day-to-day, lower profile instances of inappropriate content regulation is unknown, partly as a result of the lack of any meaningful transparency about moderation decisions from the online platforms themselves. This lack of transparency also reinforces the difficulty of ensuring awareness of when and why mistakes have been made.

21. Earlier this year, GPD developed a model for how platforms can regulate content in a human rights-respecting manner through their Terms of Service. The model we propose can be divided into three stages: (i) the development of Terms of Service, (ii) their implementation, and (iii) the provision of a grievance and remedial mechanism. It is the case that many online platforms are already compliant with some aspects of the model; however, no platform is fully compliant with the model as a whole. The model proposed specifically addresses question 3 in that it would ensure online platforms are effective, fair and transparent when moderating content, and includes processes for individuals who wish to reverse decisions to moderate content. The model also addresses question 5 in that it sets out the responsibilities of online platforms to protect the right to freedom of expression when moderating content.

(i) Developing Terms of Service

22. From a human rights perspective, Terms of Service serve two particular purposes. First, they make clear what forms of content the platform will remove or restrict, allowing for comparison with the justified limitations on freedom of expression under international human rights law. Second, they enable users to know, with a reasonable degree of confidence, under what circumstances content they wish to make available will be removed or restricted, ensuring transparency and certainty. Terms of Service may also include other aspects of the platforms' operations, or its relationship with its users and third parties. They may be titled as 'Community Standards', 'Community Guidelines', 'Content Policy' or something else. Here, we use 'Terms of Service' as a catch all, referring to the platform's rules relating to content.

23. We believe that the development of Terms of Service is not just beneficial, but a responsibility of platforms under international human rights law and the Guiding Principles. The right to freedom of expression includes online expression as well as offline expression.[781] Principle 11 of the Guiding Principles provides that

[778] Browne, M., "YouTube Removes Videos Showing Atrocities in Syria", *The New York Times*, 22 August 2017.

[779] BBC News, "Qatar's Al Jazeera Twitter account back after suspension", *www.bbc.co.uk*, 17 June 2017, available at: http://www.bbc.co.uk/news/world-middle-east-40311882; Solon, O., "Two cases of Twitter abuse highlight the obscure nature of suspensions", *The Guardian*, 10 January 2017.

[780] TIME, "The Story Behind the 'Napalm Girl' Photo Censored by Facebook", *time.com*, 9 September 2016, available at: http://time.com/4485344/napalm-girl-war-photo-facebook/.

[781] Human Rights Committee, *General Comment No. 34: Article 19: Freedoms of opinion and expression*, UN Doc. CCPR/C/GC/34, 12 September 2011, 2011, Para 11.

"business enterprises should respect human rights" and that this means that "they should avoid infringing on the human rights of others". We believe that, taken together, these two principles mean that platforms – in order to ensure a consistent degree of protection of human rights – have a responsibility not to restrict freedom of expression exercised via their platforms in a way which is inconsistent with international human rights law and standards.

24. Under international human rights law, restrictions on freedom of expression are only permissible when they are "provided by law" (to use the wording in Article 19). This means that any restriction must be "formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public".[782] While Article 19 was drafted to set out the obligations of states, we believe that the responsibility of businesses to respect human rights is best met through having the same principles applied to them, as far as possible. As such, we believe that platforms should not restrict freedom of expression unless the restrictions are "made accessible to the public" and "formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly". This, in essence, is what Terms of Service should do.

Availability and accessibility

25. Terms of Service should be easily accessible for users both during use of the platform and, where registration is required, at the point at which the user signs up to the platform. While it is, of course, up to the user to decide whether and when to review a platform's Terms of Service, the platform should take reasonable steps to make users aware of their existence. They should not be contained in a long, dense user agreement; nor should they be difficult to find on the platform's website. Instead, they should be published as a self-contained resource, and be quickly and easily accessible on the platform's website. In addition, the Terms of Service should, as far as possible, be in plain language and accessible formats, and available in the languages that their users understand. Where they are revised, users should be notified in advance of the changes being made.

Sufficient precision

26. Because of the need under Article 19 for "sufficient precision" when restricting freedom of expression, only setting out the types of content that will be moderated in any Terms of Service would not be enough to meet the requirements of the first criterion for permissible restrictions under Article 19. States, for example, would meet this obligation through specific legal provisions of general applicability, accompanied by some form of elaboration (e.g. explanatory notes published alongside legislation, guidance from relevant government departments, or guidance from the police or prosecution authorities). Interpretation of terms by courts can also help provide clarity on the circumstances when particular forms of expression will be prohibited. We believe that platforms should provide an equivalent degree of clarity so that

[782] *Ibid*., Para 25.

users are able to regulate their conduct (i.e. the content they upload, generate and seek to access) accordingly. This means that as well as developing Terms of Service, platforms should ensure that they provide sufficient detail – whether through accompanying documents or in the Terms of Service themselves – to enable users to know, with a reasonable degree of certainty, whether particular content is or is not restricted.

27. In practice, the Terms of Service which platforms have so far developed tend to set out broad categories of the different forms of unlawful or harmful content which they prohibit; for example, 'hate speech' or 'graphic violence'. We support the categorisation of forms of unlawful and harmful content. We detail possible categories later on in this submission and propose a triaging procedure for platforms when responding to content which has been flagged, using these categories to help determine how to respond. However, regardless of which broad categories of restricted content are used, there are a range of ways that this "sufficient precision" criterion can be met:

- Platforms could simply provide more detailed interpretation or guidance in the Terms of Service themselves.

- If platforms have concerns that this would make the Terms of Service too long or complex, they could retain broad, simple categories in the Terms of Service with more detailed interpretation or guidance available via a link.
- Platforms could also provide examples, either hypothetical or based on real instances, of content that would or would not be restricted under each category.

Categorisation of the forms of restricted content

28. As well as a requirement that any restrictions on freedom of expression be "provided by law", Article 19 of the ICCPR also requires that they be for one of a number of specified purposes, namely (a) for respect of the rights or reputations of others, or (b) for the protection of national security or of public order, or of public health or morals (the permissible limitations set down in Article 19(3)).

29. International human rights law also requires the prohibition of certain forms of expression: Article 20 of the ICCPR prohibits propaganda for war and advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. The Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (ratified by the UK in 2009 prohibits, among other things, images of child sexual abuse.

30. We believe this has two key implications for platforms:

- First, they should restrict content which constitutes propaganda for war; advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence; or child sexual abuse.

- Second, if they are to restrict any further forms of content, such restrictions should be necessary and in pursuance of one of the legitimate aims set out in Article 19(3), i.e. to ensure respect for the rights or reputations of others, or for the protection of national security, public order, public health or public morals.

31. While none of these forms of expression in the first group are defined within the relevant treaties themselves, sources of interpretation and guidance exist. The 2011 report of the former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, for example, provides guidance on the interpretation of these and other forms of expression which are prohibited under international human rights law.[783]

32. In relation to the second, while these legitimate purposes are broadly worded in Article 19(3), there are also sources of interpretation and guidance as to how they apply to different types of expression. The UN Human Rights Committee's General Comment No. 34, for example, provides further interpretation and clarification of each of the legitimate aims, and they have also been considered in the jurisprudence of cases brought to the Human Rights Committee on the basis of a violation of Article 19. The General Comments and Recommendations of other UN Treaty Bodies, as well as decisions of other regional and national courts interpreting equivalent provisions protecting the right to freedom of expression, are also illustrative.

33. The nine categories below are typical of the most common forms of restricted content contained within major platforms' existing Terms of Service. All would, fully or partially, correspond to one or more of the legitimate aims in Article 19(3).

Category of content	**Legitimate aim**
Threats or incitement of violence (or other harm to a person or property)	The rights or reputations of others
Facilitating other criminal activity	The rights or reputations of others; protection of public order
The glorification of, or support for, terrorism or organised criminal activity	Protection of national security; protection of public order
Bullying or harassment of other users which does not amount to a criminal offence	The rights or reputations of others
Hate speech against particular groups	The rights or reputations of others
Child sexual abuse	The rights or reputations of others
Adult sexual content	The rights or reputations of others; protection of public morals
Violence and other graphic content	Protection of public morals

[783] UN General Assembly, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc. A/66/290, 10 August 2011. See, in particular, Paras 20-36.

Copyrighted and trademarked material	The rights or reputations of others

34. If platforms propose to restrict content which does not fall into these categories, we believe that they should only do so if it would be consistent within one of the legitimate aims set out in Article 19(3). However, even some of these categories, as a result of their breadth, potentially include both content which is and is not unlawful or harmful. For example, 'adult sexual content' could include pornographic videos which a platform could legitimately restrict, but also images of naked adults, or genitalia, which have an artistic or scientific basis, and ought not to be restricted. As such, it is important that the interpretation or guidance which accompanies the Terms of Service makes it clear that content which does not fall into the exceptions set out in Article 19(3) will not be restricted, even where it falls within the broad category of content.

35. We recognise that there may be situations where platforms have been (or may be) developed for a specific purpose, or for a particular community, which needs restrictions on certain content to ensure that the platform can meet the legitimate needs of its users. For example, a platform which is developed exclusively for children may want to restrict mildly violent or graphic content which a platform developed for adults would not. Or a platform developed to provide a safe space for a particular minority group, or a vulnerable or marginalised community – such as LGBT individuals or those with mental health problems – may wish to restrict content which, while not offensive, indicates opposition to LGBT rights, or which could trigger anxiety or panic among those with a particular mental health condition.

36. In such circumstances, we consider that such restrictions would fall within the legitimate aim of 'the rights of others'; with 'others', in this case, referring to the users for whom the platform was designed. Where, however, a platform considers that its specific purpose, or the community that it has been developed for, justifies particular restrictions on content, it should ensure that any such restrictions are both "necessary" and as narrowly drawn as possible while still meeting their users' legitimate needs.

Multistakeholder engagement in development and review

37. There are a number of benefits for platforms that can be derived from consulting and engaging with a broad range of relevant stakeholders during the development of the Terms of Service. This engagement can bring expertise to the process, and boost confidence in, and the legitimacy of, the Terms of Service which are ultimately developed.

38. Given the generally global application of a platform's Terms of Service, it is even more important that relevant expertise on particular issues be harnessed to ensure that the final Terms of Service are fit for purpose. The wide range of users, on linguistic, religious, cultural and other grounds, means that a platform is unlikely to have all of the necessary expertise to be able to develop Terms of Service which can apply globally and fairly.

39. Platforms should therefore engage with all relevant stakeholders and representative and interest groups in developing their Terms and Service and

accompanying interpretation and guidance. The precise stakeholders and groups with which the platform should engage will vary depending on the particular form of unlawful or harmful content which is being considered but may include:

- Experts in freedom of expression generally (such as academics or human rights organisations);
- Groups advocating on behalf of particular vulnerable or marginalised groups, such as women, children, persons with disabilities, LGBTI individuals, ethnic and religious groups;
- Law enforcement agencies;
- Experts in terrorism and radicalisation;
- Linguistic experts;
- Psychologists.

40. For example, developing Terms of Service and accompanying interpretation and guidance on what constitutes child sexual abuse may require consulting experts on international law (particularly the Convention on the Rights of the Child and its Protocols), children's rights groups, and international or national law enforcement agencies.

41. Terms of Service and accompanying interpretation and guidance should be periodically reviewed to ensure that they remain fit for purpose, and be revised and updated as necessary.

(ii) Implementing Terms of Service

Pre-emptive and proactive restriction and removal of content

42. The model we propose for implementing Terms of Service is one to be used only after content has been published and brought to the attention of the platform as potentially in breach of its Terms of Service. There are calls, particularly from governments, for platforms to restrict content from being made available even before it is published ('pre-emptive moderation') and to proactively monitor content on the platform ('proactive moderation'). Some platforms already undertake either or both of these.

43. With regards to pre-emptive moderation of content, we recognise that there may be certain very limited circumstances where decisions to moderate content prior to publication could be made by a platform consistently with international human rights law and standards. However, these are limited to those where (i) specific content has already been identified by a human as unambiguously and, regardless of context, in breach of international human rights law (and therefore also the platform's Terms of Service if our model is followed), such as images or videos of child sexual abuse, and (ii) it is a copy of such content that a user has sought to share.

44. Where automatic processes are able to identify content which is a copy of content a platform has already decided should not be published, it is logical for that process to prevent its further publication. There are examples of this process taking place already, such as the Internet Watch Foundation in the UK, which has developed an Image Hash List comprising hundreds of thousands of hashes of images of child sexual abuse. This hash list is updated daily and distributed to companies who pay for the service. These companies are then able to use these hashes both to identify images of child sexual abuse which have already been uploaded, and to prevent them from further being uploaded at all.
45. While an example of best practice, the use of such a process is limited to circumstances where the content is a copy of already identified content, and that content is unambiguously in breach of international human rights law (and so the Terms of Service), regardless of context or other factors. Its utility does not extend to the moderation of content which is new, where the content is not clearly unlawful or harmful, or where context is a relevant consideration. While such a model could therefore potentially play a part in preventing, for example, the publication of copyrighted material in certain circumstances, it is difficult to conceive of other forms of content where it could play a role.

46. As such, and subject to those certain, limited exceptions, we do not consider that platforms should moderate content prior to publication. As well as the risks to freedom of expression given the absence of the safeguards attached to the model proposed in this section, there are also reasons of practicality. The sheer volume of content which is uploaded for publication makes it almost impossible for it all to be pre-emptively moderated by a platform. The number of people and amount of time required would far exceed the capacity of even the most well-resourced platforms, and would entirely undermine the instantaneous nature of content uploading and sharing. As it is only ever a small proportion of content which is unlawful or harmful, we believe it is preferable for platforms to focus their resources on content which has been flagged as such, rather than to monitor all content prior to publication.

47. With respect to proactive moderation of content, the same considerations of scale and practicality apply. However, we note that many platforms are already proactively moderating content, often through the use of algorithms and automated processes. Between October and December 2017, for example, YouTube removed over 6.6 million videos identified as in breach of its Community Guidelines following an automated flagging process.[784] Where platforms do proactively moderate content, the same stages set out below should be followed once content has been flagged as a result of that internal review.

The role of algorithms and automated processes

48. The sheer scale of content which is uploaded online each day is vast, and it would be infeasible for the entire content moderation process to be undertaken by humans. It is understandable that platforms have therefore turned to the use

[784] YouTube Community Guidelines enforcement, available at: https://transparencyreport.google.com/youtube-policy/overview.

of algorithms and automation to identify potentially unlawful or harmful content. However, there are mixed opinions on the benefits of using algorithms and automated processes for such purposes, and demonstrable risks to freedom of expression.

49. One example where automated processes have shown to be successful is the use of hashes by the Internet Watch Foundation in the UK, as detailed above at paragraph 44. As well as the clear and objectively unlawful and harmful nature of the content, it is important to note that there is still human oversight of the process, in that analysts check each child sexual abuse image before hashing it and adding it to the Image Hash List. As such, the automated process only kicks in after a particular image has been reviewed by a human, and only applies to that image and copies of it.

50. Outside of this narrow field, however, the benefits of algorithms and automation are, at least at present, less well established. Indeed, there is clear evidence of the limitations that currently exist in using automation and algorithmic filtering to regulate content. In its recent report, 'Mixed Messages: The Limits of Automated Social Content Analysis',[785] the Centre for Democracy & Technology highlighted a number of substantive limitations to these automated processes in the context of social media platforms. These included:

- The varying levels of reliability in identifying harmful content given significant differences in language use across different platforms, by different demographic groups and depending on the topic of conversation.

- The risk of decisions based on automated social media content analysis further marginalising and disproportionately censoring minority groups and those that face disadvantage.

- The lack of any clear, well-established definitions of forms of harmful content, such as 'hate speech', 'extremist material' or 'radicalisation', which are necessary for effective automated content analysis.

- Differences between what the coders of the tools themselves considered as falling into the categories, often as a result of different cultural backgrounds and personal sensibilities.

- The inability of tools to take into account context – such as tone, the speaker, the audience and the forum – to any meaningful extent. They struggle, for example, to understand jokes, sarcasm, irony and nuance.

51. These limitations mean that any use of algorithms and automation to filter or otherwise moderate content should be considered very carefully. Although it is understandable that platforms are looking to algorithms and automation to deal with the scale of online content, there are real risks that perfectly lawful and legitimate content may be taken down, and that such moderation will

[785] Center for Democracy & Technology, "Mixed Messages? The Limits of Automated Social Media Content Analysis", 28 November 2017, available at: https://cdt.org/insight/mixed-messages-the-limits-of-automated-social-media-content-analysis/.

disproportionately impact minority groups and those that already face disadvantage. As a result any use of algorithms and automation must be accompanied by strong safeguards to mitigate these risks. In particular, we consider that three key safeguards are essential:

- First, there should always be some human oversight of any decisions made by algorithms and automation. While, of course, humans will have developed the processes and authorised their use, we believe that the results of those processes should also be reviewed by a human who will be able to act as a filter against potential removals of content which would breach the right to freedom of expression or disproportionately affect particular groups vulnerable to discrimination.

- Second, to support the procedural requirements of restrictions on the right to freedom of expression, platforms should clearly and transparently publish meaningful and easily understandable information on what processes are being used, for which purposes, and how decisions are made by those processes. This information should be available in the languages used by the users of those platforms as well as in formats appropriate for those who have learning or visual disabilities.

- Third, the algorithms and automation, and their results, should be regularly reviewed, and the processes refined, to mitigate against the risks identified above.

Flagging content

52. Regardless of any proactive moderation of content, platforms should ensure that they have the functionality allowing users to be able to notify the platform, in a simple and straightforward way, of content which they consider to be in breach of the platform's Terms of Service (flagging), thereby instigating the content moderation process.

53. For the implementation of the Terms of Service to be effective, including from the perspective of the user who published the content, it is important that sufficient information be provided so that the platform can make an informed determination of whether the content is in breach of its Terms of Service. As such, the platform should require users, when flagging content, to provide the reasons why they consider that it is in breach of the platform's Terms of Service.

54. Some platforms use a system of 'trusted flaggers', 'superflaggers' or some other mechanism by which individuals or organisations can flag multiple items of content as a result of their particular expertise or historic accuracy in potentially identifying content which is in breach of Terms of Service. If a platform decided to use such a system (and with the important qualification that such systems are not without their critics),[786] this would not negate the requirement for a final human determination.

[786] See, for example, Article 19, "EU fails to protect free speech online, again", *article19.org*, 5 October 2017, available at: https://www.article19.org/resources/eu-fails-to-protect-free-speech-online-again/.

Triaging

55. Given the wide range of forms of unlawful and harmful content that exist, and the different expertise and stakeholder engagement needed to make determinations, we propose that platforms designate distinct teams or individuals to deal with the different forms of content, using the categories developed under the Terms of Service. We would also propose that content which has been flagged should undergo a simple triaging procedure to determine which particular category the content falls most closely under, at which point the relevant team or individual will be tasked to undertake the determination process. It may be the case that this triaging procedure is also able to identify content which is manifestly and unambiguously not in breach of the platform's Terms of Service, in which case the user who flagged the content would be informed that this is the case, and the process would cease.

56. Unless the content has been identified as manifestly and unambiguously not in breach of the platform's Terms of Service, then (at the same time that the content is undergoing the triaging procedure) the user who uploaded or generated the content should be informed that the content has been flagged, and the reasons why. That user should be given a sufficient period of time to provide any information justifying why the content should not be taken down.

Provisional removal of content

57. There may be circumstances where it is appropriate for content to be provisionally removed pending the outcome of the determination process. This might apply, for example, in cases where there is a potential risk of immediate and irreversible harm were the content to remain available. In such cases, the user who generated or hosted the content should be informed. Where there is no such risk, such as where the reasons for flagging relate to copyrighted work, content should not be removed until a final determination has been made.

Determination

58. Once the content has been passed on to the relevant team or individual, a determination should then be made within a reasonable period of time as to whether the content is in breach of the platform's Terms of Service. The team or individuals should use the interpretation or guidance material developed alongside the Terms of Service. There are three additional further considerations that should be taken when platforms develop this procedure:

    - First, the platform should ensure that sufficient resources are provided to the teams and individuals making determinations, both in terms of the number of moderators and the amount of time available for moderators to make determinations.

    - Second, all staff engaged in content moderation should be given sufficient training and support in their roles. This includes not only introductory training on international human rights law and standards, and their relationship with the platform's Terms of Service, but ongoing and additional training and support where needed. The fact that content which is flagged may be disturbing – such as child sexual abuse imagery or graphic violence – means that the welfare needs of the individuals involved must be considered. Platforms should ensure that they have a rigorous recruitment process in place to ensure that the moderators recruited have the psychological and emotional capacity to undertake the work of moderating such forms of content, and provide the necessary support to moderators. This support could include shorter working hours, regular breaks, and periodic psychological and counselling sessions.

- Third, there may be circumstances where moderators need external support in order to make a decision. This could be as a result of further information and expertise being needed on linguistic, religious or cultural issues. In such circumstances, moderators should be able to – and encouraged to – seek such external expertise, with the same groups identified above as relevant to developing particular categories of restricted content within the Terms of Service.

Quality assurance

59. Platforms should introduce processes for the quality assurance of moderation decisions. This might mean inviting 'second opinions' on a selection of decisions to ensure accuracy and consistency; reviews of moderators' decisions and the proportion that are overturned after a second opinion or after an appeal; external review by the groups identified earlier of decisions that are made by moderators; or using 'mystery shoppers' to test the moderation procedure from a user's perspective.

Communication of determination

60. The outcome of the determination should be communicated both to the user who flagged the content and the user who uploaded or generated the content, along with reasons for the determination and – if the content has been determined to be in breach of the platform's Terms of Service – the available grievance mechanism.

(iii) Grievance and remedial mechanism

61. However well-developed and implemented a platform's Terms of Service may be, mistaken or inappropriate removal of content is inevitable. Such mistaken or inappropriate removals may, however, constitute an adverse impact on the user's right to freedom of expression. The Guiding Principles address this situation, with Principle 22 making clear that where a business identifies that they have caused or contributed to an adverse impact, they should provide for or cooperate in their remediation through a legitimate process. This responsibility reflects the well-established principle in international human rights law that those who have suffered a human rights violation are entitled to an "effective remedy".[787]

[787] See, for example, Article 2(3)(a) of the ICCPR which requires states to ensure that any person whose rights of freedoms are violate has an effective remedy.

62. The Guiding Principles also set out in some detail how such a remedy should be provided. Principle 29 states that businesses should "establish or participate in effective operational-level grievance mechanisms for individuals and communities who may be adversely impacted". Principle 31 goes on to set out a number of criteria for a grievance mechanism to be effective.

63. In the context of content regulation, platforms should establish a grievance mechanism which (i) requires the user to be informed that the content has been removed (or that the platform proposes to remove that content, or that their account has been suspended, as the case may be), (ii) provides an opportunity for the user to challenge that decision, and (iii) provides an effective remedy where the challenge is successful. We further believe that such a grievance mechanism can meet these requirements by fully complying with the criteria set out in Principle 31 of the Guiding Principles.

- **Legitimate**: The principle of legitimacy requires that the stakeholder groups impacted have trust in the process, and that there is accountability for its fair conduct. Platforms should involve relevant stakeholders in both the design of the grievance mechanism and – where appropriate – in its implementation; for example, by involving the groups identified above in reviewing decisions that have been made by moderators and appealed.

- **Accessible**: The principle of accessibility requires that the grievance mechanism is known to the stakeholders who would need to use it, and that adequate assistance is provided for those who may face particular barriers to access. It should be clear on the platform how a user can challenge a decision which has been made to remove content or to suspend their account. Users should always be informed when their content has been removed or their account suspended. When informing the user, clear information should be given on how the user can appeal the decision. Platforms should also consider barriers which may exist for a user to appeal the decision and engage in the grievance mechanism, such as language or disability.

- **Predictable**: The principle of predictability requires that there be a clear and known procedure with an indicative time frame for each stage, and clarity on the types of process and outcome available and means of monitoring its implementation. Platforms should set out publicly what the review process is if a user challenges a decision to remove content or to suspend their account. The information should also set out an indicative time frame and what the available remedy (or remedies) will be if the appeal is successful.

- **Equitable**: The principle of equity requires that aggrieved parties have reasonable access to sources of information, advice and expertise necessary to engage in a grievance process on fair, informed and respectful terms. Platforms should ensure that users who have had content removed or their account suspended are informed of the full reasons for the decision.

- **Transparent**: The principle of transparency requires that parties are informed about the progress of the grievance mechanism and provided with sufficient information about the mechanism's performance to build confidence in its effectiveness. Platforms should ensure that users who appeal against decisions to remove content or suspend their account are informed about the progress of the appeal at regular intervals. It also means that platforms should publish details on the grievance mechanism and how appeals are determined.

- **Rights-compatible**: The principle of rights-compatibility requires that outcomes and remedies are consistent with internationally recognised human rights. Platforms should ensure that the available remedies if a user is successful in appealing a decision are effective. Ordinarily, the most effective remedy will be the reinstatement of the content or the account, as the case may be. Depending on the circumstances, other remedies may also be appropriate, such as compensation, a public apology, a guarantee of non-repetition, or a review/reform of a particular policy or process. Remedies should not, themselves, constitute an adverse impact on users' human rights: for example, public apologies about inappropriate or mistaken decisions should not identify the user concerned without their consent, or otherwise interfere with their privacy.

- **A source of continuous learning**: The principle of continuous learning requires that that there be regular analysis of the frequency, patterns and causes of grievances to enable the institution administering the mechanism to identify and influence policies, procedures or practices that should be altered to prevent future harm. Platforms should regularly review the frequency, patterns and reasons for appeals against the removal of content or the suspension of accounts, to identify whether any steps need to be taken in reviewing or reforming internal policies and processes to avoid future inappropriate or mistaken decisions.

- **Based on engagement and dialogue**: The principles of engagement and dialogue require that there be engagement with affected stakeholder groups about the design and performance of the grievance mechanism, and recommend a focus on dialogue as the means to address and resolve grievances. Platforms should ensure that they engage in regular dialogue with stakeholder groups once the grievance mechanism has been established in order to identify any barriers to continued confidence.

64. Finally, under no circumstances should a platform's grievance mechanism exclude the possibility for a user to use alternative state-based grievance mechanisms, such as judicial processes or complaints to a national ombudsman.

Oversight

65. Question 3 also asks who should be responsible for overseeing content moderation processes as well as appeals. While this should primarily be the role of the online platforms themselves, concerns over seemingly arbitrary and non-transparent decisionmaking by platforms has resulted in further criticism have raised the question of whether some further mechanism of regulation or oversight is needed.

66. The question of whether – and to what extent – a particular sector, industry or profession needs to be regulated is a complex one which requires consideration of many different factors. At one end, there are sectors and services which

provide public functions or exercise power or influence such that there is a clear public interest in regulation. Examples include law enforcement agencies or health professionals who may be employed and regulated directly by the government. At the other end, there are sectors and services which are entirely private in nature, or who have a minimal impact upon individuals, meaning that little or no regulation is required, beyond horizontal regulation such as consumer rights or health and safety legislation. Between these two extremes lie a range of different sectors and services which have differing levels of regulation, including self-regulation or co-regulation.

67. We believe that there is a clear public interest in the activities of online platforms and the services that they provide. As we note at the start of this submission, many platforms have millions, if not billions of users, and the services offered are becoming increasingly important and essential in the lives of those users. It is widely accepted that utilities like water, electricity and telephony are recognised as so important to day-to-day life that companies engaged in making them available are not left entirely to market forces and self-regulation. Increasingly, there is a case for treating the internet – and, by extension, the platforms which make up people's experience of the internet – in the same way. As we also note at the start of this submission, platforms are becoming increasingly important in enabling individuals to exercise their right to freedom of expression, with the actions of those platforms via content regulation potentially impacting adversely upon that right.

68. These factors suggest that a purely self-regulatory mechanism is not sufficient to ensure that the interests of users – and the public interest more broadly – is adequately protected. Existing means of accountability for the actions of platforms via investors and stakeholders appear to have little impact. The major voluntary industry-level initiative, the Global Network Initiative (GNI), takes a soft-touch approach – setting out fairly high-level principles in the GNI Principles and Implementation Guidelines, and refraining from publishing full assessments of company members' compliance with them.

69. As such, we do not believe that the existing mechanisms ensure a sufficient level of protection for the interests of users, including their human rights. While the model we propose above, if fully implemented, would help ensure a sufficient level of protection for the right to freedom of expression, we judge that pure self-regulation would not provide the necessary transparency, accountability and representation of the public interest. We therefore believe that an additional oversight mechanism should be established to provide that transparency, accountability and representation of the public interest.

70. We do not, however, believe or propose that such an oversight mechanism should be developed by governments and implemented through national legal or regulatory frameworks. This is for two reasons. First, the global nature of platforms makes national-level mechanisms inappropriate, creating the risk of platforms being forced to comply with scores of different requirements when the issues and interests at stake are global in nature and importance. Second, given the poor human rights record and high levels of censorship in many countries, national level regulation or oversight on issues of content would create significant risks to freedom of expression in those countries.

71. We believe that there is a middle ground between the current purely self-regulatory approach and the development of national-level regulatory or oversight mechanisms. We propose a new, global model of oversight which combines a set of independently developed standards with a multistakeholder mechanism for enforcement. We recognise that there are few, if any, comparable models in other sectors, and that this would be a radical step forward. As such, we have confined our proposals for such a mechanism, at this stage, to relatively high levels of principle, rather than detail.

Developing the oversight mechanism

72. In the first instance, we propose that interested platforms establish an independent group of experts and set out a Terms of Reference for it to develop the Online Platform Standards (the Standards). The Standards would contain both minimum requirements for platforms as well as an oversight mechanism as detailed below. This group should comprise experts on the relevant issues, including international human rights law, business and human rights, and the operations of platform themselves. In developing the Online Platform Standards, the group of experts should consult with platforms and other interested stakeholders, such as academia, civil society and investors.

Framework underpinning the new oversight mechanism

73. We propose that the Terms of Reference should provide for the Online Platform Standards to include the following:

- **Establishment of the OPSO and the Standards**: A global body, the Independent Online Platform Standards Oversight Body (OPSO), would be established, governed by the Standards and by which participating platforms would publicly acknowledge themselves bound. The OPSO would be funded by participating platforms themselves. Any further platform would be able to sign up to the Standards at any time.

- **OPSO membership**: The Standards would set out that membership of the OPSO would comprise a voluntary, multistakeholder group comprising representatives of the platforms, civil society organisations, academia and, potentially, relevant national bodies.

- **Minimum standards**: As well as establishing the OPSO, the Standards would include a commitment from the participating platforms to develop and implement a human rights-respecting framework for content regulation, based on a set of minimum requirements contained within the Standards. These minimum requirements would go beyond the level of principle, and provide detail on the development of Terms of Service, their implementation, and the provision of grievance and remedial mechanisms. We would recommend that our proposed model, set out above, be considered as the framework, adapted by the platforms as necessary.

- **Standardisation of forms of content**: The Standards could also, where possible, set common categorisations, definitions and understandings of the different forms of unlawful and harmful content which would be subject to restriction. This would promote standardisation and consistency, providing benefits for users themselves when they use multiple platforms, and helping platforms achieve greater efficiency in content moderation and comparison.

- **Support**: The Standards could also provide for platforms to be able to seek advice and assistance from the OPSO on particular issues.
- **Review and amendment**: The Standards would be reviewed periodically (and no less frequently than biennially) to ensure that they remain fit for purpose. Any amendments to the Standards would be developed by independent experts, as with the original Standards, following a process of multistakeholder consultation, including with platforms.
- **Enforcement**: Enforcement of the Standards would be undertaken by the OPSO. The Standards would provide that the OPSO would have the authority to assess, at periodic intervals, compliance by the platforms with the Standards. The Standards would require platforms to provide all necessary assistance to the OPSO to be able to carry out its functions, including by providing details on their compliance.
- **Transparency**: To improve transparency, the Standards would empower the OPSO to publish reports, and make them publicly available, on compliance by the platforms with the Standards, following each assessment. The reports would also contain recommendations for change to ensure compliance.
- **Non-compliance**: We do not propose that the Standards should give the OPSO any power to sanction platforms for non-compliance with the Standards. Instead, the reports published by the OPSO would contain a clear assessment of whether, and to what extent, the platforms were acting in compliance with the Standards. The reports would also contain recommendations on how non-compliance should be remedied. The Standards could provide for the suspension or expulsion of a platform which repeatedly failed to comply with the Standards.

74. Although, as noted above, we do not propose any national level regulation of platforms, we nonetheless recognise that there exist a number of national level bodies who have a particular interest in online content regulation. These include national human rights institutions (NHRIs), such as the UK-based Equality and Human Rights Commission who have a clear interest in the protection and promotion of human rights at the national level, but also bodies such as the Internet Watch Foundation (in the UK) and the eSafety Commissioner (in Australia) who have mandates to undertake certain functions relating to the regulation of unlawful or harmful content at the national-level. The OPSO should seek to work closely with NHRIs and other bodies with national-level mandates, such as through Memorandums of Understanding.

Question 6: What information should online platforms provide to users about the use of their personal data?

75. Article 17 of the ICCPR guarantees the right to privacy which, as has been confirmed by the UN Human Rights Committee, includes protection of personal

information.[788] This means that "every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes".[789] Other international standards provide greater detail about the minimum standards that any human rights respecting data protection framework should provide, primarily the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and Council of European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), which the UK ratified in 1987.

76. The data protection framework in the UK (the Data Protection Act 1998, soon to be superseded by the EU General Data Protection Regulation) provides a high degree of protection for individuals when it comes to their personal data, however there remains a degree of confusion among users as to what personal data is being collected by online platforms and for what purposes; the degree to which users are given the opportunity to provide informed and meaningful consent to the collection and use of their personal data has also been questioned.[790]

77. While most, if not all, platforms will have a 'privacy policy' or 'data protection' policy, these by and large do not facilitate fully informed and meaningful consent. This stems from a number of factors: first, people rarely read these policies when signing up to a platform or as a user; second, when people do read them, they do not always understand them; third, even if they read and understand them, there is rarely any choice given as to different levels of consent with platforms more often than not offering a single 'take it or leave' it option.

78. There are a number of steps that online platforms should take to ensure that users are able to provide informed and meaningful consent to the collection, storage and use of their personal data, drawn from a range of best practice documents, in particular the recommendations set out in of the Ranking Digital Rights Corporate Accountability Index 2018,[791] the Article 29 Working Party (WP29) guidance on consent,[792] the Information Commissioner Office code of practice on privacy notices,[793] and draft guidelines on obtaining meaningful

[788] UN Human Rights Committee, *General Comment No. 16: Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation)*, 1988, Para 10: "The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law."

[789] *Ibid*.

[790] See, for example, the Ranking Digital Rights Corporate Accountability Index 2018 which reviewed 22 of the world's world's most powerful internet, mobile, and telecommunications companies on their public commitments and disclosed policies affecting users' freedom of expression and privacy, available at: https://rankingdigitalrights.org/index2018/. The report found that users "lack the information they need to make informed choices to assess the privacy and human rights risks they face when using a particular service" and that companies "did not sufficiently disclose what user information they share and with whom, for what purposes they collect and share this information, for how long they retain it, and what options users have to control whether information about them is collected and shared".

[791] Ranking Digital Rights Corporate Accountability Index 2018, available at: https://rankingdigitalrights.org/index2018/report/privacy-failures.

[792] Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679*, 28 November, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

[793] Information Commissioner Office, *Privacy notices, transparency and control: A code of practice on communicating privacy information to individuals*, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control.

online consent developed by the Office of the Privacy Commissioner of Canada.[794]

79. First, the privacy policy should be written clearly, in plain language and available in accessible formats. They should not be contained hidden within dense user agreements, but as self-contained policies brought to the specific attention of users when registering for platforms. They should also be prominently displayed on the platforms themselves so that existing users are able to access them quickly and easily. While the full policy should be available, it may be the case that certain elements need greater attention or emphasis to ensure that consent is meaningful. Summaries of particular aspects may be useful, but users should be able to decide if they want more detail.

80. Second, those policies should contain information on precisely what personal data is *collected* by the platforms, for what purposes, and for how long. They should also contain information on precisely what personal data is *shared* by the platforms and the names of the third parties with whom it is shared.

81. Third, users should be given clear options to control what information is collected and shared, including for the purposes of targeted advertising. In particular, platforms should ensure that users are provided with easy 'yes' or 'no' options when it comes to the collection, use or sharing of personal data which is not essential to the product or service that the platform offers. Options should not nudge users towards a particular decision, for example, by using different sized fonts and colours, more prominently displaying one option over another. Users should be able to change their consent settings at any time.

82. Fourth, platforms should also clearly disclose if and how they track users and non-users across the internet using cookies or other tracking tools which are embedded on third-party websites.

83. Finally, platforms should also make clear how users can obtain a copy of all personal data which has been collected and stored, as well as to request that information which is inaccurate or no longer relevant to the platform's purposes be corrected or deleted.

Question 7: In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

84. We have addressed the issue of transparency of online platforms in our responses to the questions above, particularly in paragraphs 25 to 27 (regarding online platforms' Terms of Service and content moderation processes), paragraph 51 (regarding their use of algorithms) and paragraphs 79 to 83 (regarding online platforms' use of personal data).

May 2018

[794] Office of the Privacy Commissioner of Canada, Draft guidelines: Obtaining meaningful online consent, available at: https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-consent-under-pipeda/gl_moc_201709.

Google UK - written evidence (IRN0088)

Executive summary

1.1 Google welcomes the opportunity to provide comments on the House of Lords Communications Committee's inquiry into regulation of the internet. The inquiry and the evidence that the Committee gathers will provide a timely and valuable contribution to the debate on online regulation. Now 20 years old, Google has grown from a start-up in a garage to a global company that complies with legal obligations in all the countries we operate in and works hard to protect our platforms from abuse. We are keen to work constructively with government to build on the existing legal framework and to build trust and confidence in the systems and procedures that ensure online safety.

1.2 It is important to note from the outset that the internet is far from the 'wild west' some claim it is and the current publisher vs platform debate is oversimplified. We operate in an environment where extensive regulation of online content and actions already exists and is being enforced. Much of the regulation for conduct online is equivalent to that which applies to offline conduct, with some additional protections applicable specifically to the online context. From the Consumer Rights Act to the new EU Audiovisual Media Services (AVMS) Directive or the Competition and Markets Authority (CMA), online behaviours come under the scope of a diverse and evolving set of legislation, multi-stakeholder initiatives and regulators.

1.3 We want to maintain an open and constructive dialogue with government and other stakeholders on how methods and responsibilities to tackle potential harm are changing. It is right that as our platforms and technologies evolve, we continue to invest in developing more efficient systems to address problematic content online. This submission sets out our view on what industry best practice and governance should look like and how this can effectively build on top of the existing regulatory framework.

1.4 The UK's vibrant digital economy is a growth engine for the country and a recognised world-leader. The turnover of digital tech businesses in the UK reached £170 billion in 2017 - an increase of £30 billion in just five years[795]. E-commerce - the buying and selling of goods online - and the growth of online platforms have been key components of this success: in 2017, 77% of adults bought goods or services online, and 66% used social media for networking purposes[796]. Platforms like YouTube are an important source for education and access to information while also giving budding artists an outlet for their creativity and entrepreneurialism and a platform for global cultural export. We are proud to see that 85% of all YouTube views on videos uploaded by a UK-based creator are by viewers watching from outside of the country[797], evidencing Britain's growth as a global influencer.

1.5 Open platforms such as Google have ensured that everyone, from a child in rural India to a university professor in Oxford, has access to the same rich information

[795] https://technation.techcityuk.com/

[796] https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2017

[797] YouTube internal data, 2018

available online, while creators and businesses of all sizes have the same opportunities to find customers and fans across the globe. User generated content, which ranges from comments and reviews, to videos or blog posts, has played a significant role in creating the rich and diverse web we have today. We are proud to help power this part of the digital and creative economy but also recognise there is a challenge to this openness; some bad actors with ill intentions attempt to exploit our platforms, seeking to mislead, manipulate, harass or even harm.

1.6 The legal framework setting out platforms' responsibilities, underpinned by the e-Commerce Directive (ECD) has been effective in navigating this challenge. The internet is a complex ecosystem and relies upon the collaboration of multiple players including, but not limited to, users, content creators, Internet Service Providers, domain owners, hosting providers, advertisers, etc. The current framework provides a robust regime for responsibility and action, whilst also protecting a free and open internet. It balances the interests and responsibilities of all of these players - supporting transparent, responsible and informed sharing of user generated content. It ensures that those who post material online take responsibility for the content that they produce whilst also fixing platforms with a clear responsibility to act if they are notified of illegal content.

1.7 The ECD has the advantage of setting out different requirements for different types of intermediaries, rather than being aimed at a particular business activity. It has led to the growth of a wide variety of services and business models, and is flexible enough to cover the multiplicity of activities and content types online. For example, an online news site can contain content authored by the news organisation, along with material licensed from third parties and user-generated comments - the news site will be directly responsible for the editorial content it publishes, but will have different legal responsibilities with respect to user comments that the website is hosting as an intermediary. This online intermediary liability regime has fostered the huge economic and cultural benefits of the internet while ensuring platforms are taking appropriate and speedy actions in removing unlawful content.

1.8 It is important to note that the flexibility and nuance of the ECD's platform responsibility provisions have allowed companies like ours to continue to invest in innovative ways of tackling harmful content online. Whether it's developing a state of the art content management system for copyright owners through Content ID on YouTube, or the use of machine learning to help identify violent extremism content, we are always looking for ways to more effectively and efficiently carry out our responsibilities. This work augments our notice-and-action model and builds upon our strong cooperation with law enforcement, trusted flaggers and our community of users.

1.9 But it is not just technology that changes. The rules governing online content are also far from static, and are evolving to keep pace with online change. Last year, Google signed a copyright code of practice supervised by the Intellectual Property Office (IPO) that brought together search engines and the creative industries to tackle online piracy, and introduced an independent audit of the effectiveness of our search anti-piracy tools. Later this month the GDPR will be implemented across the EU, including in the UK, forging a new standard in data protection regulation that will significantly boost consumer and privacy protections. Industry is also working with the government on the development of its Digital Charter, while bodies such as the Advertising Standards Authority (ASA) remain active in enforcing standards online.

1.10 Of course, we recognise that given the fast moving nature of the internet, it is important for policymakers and interested stakeholders to continue to have ongoing conversations with industry about new areas of collaboration and to facilitate discussions on improvements that can be made to the existing frameworks to ensure they remain fit for purpose.

1.11 However, we believe caution needs to be applied when considering any changes that could adversely affect the fundamental principles that underpin the online ecosystem. Drastic reform of the ECD provisions that strike a careful balance between the interests of persons affected by unlawful information, internet intermediaries and internet users, will not only undermine the benefits of the current system (which we detail in our submission), but also creates several unintended and damaging consequences. Shifting liability on to intermediaries for users' actions and content online would have a severe chilling effect on the access to and hosting of legitimate speech and would narrow the information and content available via the open web. Shifting liability to intermediaries may also make users, the original creators of content, less responsible for the content they are producing, therefore undermining incentives towards good online citizenship and appropriate user behaviour.

1.12 Importantly, sweeping liability reform would force platforms to pre-vet all the content that users upload, and would inevitably suffocate much of what is a vibrant digital world. A piece of content that you want to share today might take days, weeks or months before being cleared for publication. It would undermine the ability of British citizens to create content and participate in online communities – to share information, education and entertainment – in marketplaces, and in activities that have been such a boom for the economy. As a first-mover, the UK would damage its competitiveness through diverging with well-established EU-wide regulation, and by falling far out of step with global norms.

1.13 It is, therefore, critical that any proposals for reform are carefully evaluated and consulted upon and are surgically targeted with the aim of strengthening the partnership between the law, the public and the platforms in rooting out unacceptable content or preventing the identified harm.

1.14 The societal advantage of the current ECD platform responsibility provision is that it not only provides a solid baseline framework which companies can use in order to scale up or innovate their content moderation tools, but it also allows for new flexible institutional responses to be built on top of it. The UK has the opportunity to look at and potentially expand internet governance models that have already been tried and tested. The UK industry and policymakers already have an internationally acclaimed track record for backing institutions such as the Internet Watch Foundation - which has successfully worked with industry to take down and block child sexual abuse imagery for over two decades.

1.15 Key to the success of this multi-stakeholder institution - bolstered by close cooperation with government and law enforcement - has been a clear definition of the problem that needs tackling and a strong commitment to implementation and intelligence sharing from all players involved, from ISPs to social media platforms and other types of technology companies.

1.16 The IWF and other examples of multi-stakeholder governance models such as the Global Internet Forum to Counter Terrorism, recently applauded by the Prime

Minister and the former Home Secretary, together with industry governance best practice such as clear notice-and-action procedures and transparency reports, offer an effective blueprint for helping to tackle unlawful content online; one that would avoid the pitfalls of a broad legal intervention that risks undermining free speech and the future of the digital economy.

1.17 Our submission further details our view on platforms' role and responsibilities to tackle internet harms, looking at what a good system and procedure governance framework should look like and how the government can continue to adhere to its Digital Charter goals of keeping UK citizens safe online, while also maintaining their freedom of expression, and their ability to start and grow their businesses and careers online.

Global Internet Forum to Counter Terrorism (GIFCT)

Google is a founding member of GIFCT, a multi-stakeholder initiative developed by the tech industry in collaboration with governments and non-governmental organisations, that was established in June 2017 to curb the spread of terrorist content online by substantially disrupting terrorists' ability to promote terrorism and exploit or glorify real-world acts of violence using online platforms. Building on the work started within the EU Internet Forum and the shared industry hash database, the GIFCT is fostering collaboration with smaller tech companies, civil society groups and academics, and governments.

Its members have invested heavily in proprietary and cutting-edge technological solutions such as photo and video matching and text-based machine learning classification techniques. There are now more than 90,000 hashes in the ThreatExchange Database, which allows member companies to identify and remove matching content that violates policies and in some cases block terrorist content before it's been posted.

In collaboration with the Tech Against Terror initiative — which recently launched a Knowledge Sharing Platform with the support of GIFCT and the UN Counter-Terrorism Committee Executive Directorate — the forum also held workshops for smaller tech companies in order to share best practices on how to disrupt the spread of violent extremist content online.

Question 1: is there a need to introduce specific legislation for the internet? Is it desirable or possible?

Question 2: what should the legal liability of online platforms be for the content that they host?

Existing platform responsibility laws have driven growth and helped to tackle harmful content online

2.1 The current liability regime for online platforms, established by the ECD in 2000, has facilitated the unprecedented period of creativity and engagement of the internet age. By providing platforms with clear guidance on their intermediary responsibility and protections from liability for third party content, the existing framework has helped to protect the free flow of information online and given consumers, citizens, institutions and businesses more choice, power and opportunity.

2.2 Google recognises there are challenges to openness. As we strive to counter an evolving set of bad actors on our platforms, we will continue to develop new mechanisms and we are committed to improving our effectiveness in removing illegal and harmful material. But the clear set of responsibilities and protections enshrined in the ECD allow us to continue to make technological improvements and further both freedom of expression and online safety.

2.3 We believe the current regulatory regime - supported by wider co and self-regulatory and governance interventions - has been effective in tackling these challenges without dampening the economic and cultural benefits of open and free online platforms. Among the key attributes of the current framework are:

- It creates an important balance of obligations between users, content providers and platform operators: as it stands, the responsibility for user generated content rests with the individual who creates and shares that content. Platforms, in turn, are required to swiftly respond to notifications of content that is illegal. This reinforces an important principle that Google fully supports: that people are responsible for their actions, both in the offline and online world, and platforms should invest to create safe communities.

- It incentivises significant investment in technology to tackle infringing content online: for example, Google has invested in cutting edge machine learning to allow us to quickly and efficiently review and remove content that violates our guidelines. Machine learning is helping our human reviewers remove nearly five times as many videos than they were previously. Given our investment in technological solutions, now more than half of the videos we remove from YouTube for violent extremism have fewer than 10 views. This investment is driven by our commitment to protect users and enabled by the clear protections for intermediaries - allowing us to explore new and innovative ways to use a mix of technology and human review to tackle harmful content online.

- It is adaptable to a range of digital environments: regulating activities as opposed to specific business models. This provides important flexibility in how content is regulated across different types of platforms.

The current regime is not static, and UK regulators are active in enforcing standards online

3.1 The online world is far from being an unregulated space, as online content is subject to many of the same rules and oversight as offline content. For example:

- Online advertising is held to the same regulatory standards as billboard and print advertising – ensuring that it is legal, decent, honest and truthful and that it does not mislead consumers.

- Hate speech is subject to the same laws and criminal sanctions online as it is offline.

- Anyone offering products and services online must comply with the requirements of the Companies Act and Consumer Rights Act.

- Information related to financial or medical services is subject to specific regulation that applies both online and offline.

3.2 Regulators are effective and active in enforcing these standards online. The Competition and Markets Authority has recently intervened in the cloud storage market, securing commitments from companies including Google to improve transparency around contractual terms and conditions – helping to boost service for users[798]. The CMA has also investigated compliance with consumer protection laws on car rental and hotel comparison websites.

3.3 In late 2016, the Advertising Standards Authority and Committee on Advertising Practice issued robust guidance on advertorial blogs and vlogs, ensuring that advertorial content is clearly labelled to consumers (before they view or read it) and obviously distinguishable from editorial content[799]. The ASA also regularly calls for online adverts to be amended or withdrawn if they are found to have breached their various codes of conduct.

3.4 More broadly, the Crown Prosecution Service is active in pursuing online hate crime and has issued clear guidelines on prosecuting cases involving communications sent via social media. The guidance covers a range of offences, including hate crime, intimidation, harassment and stalking, threats of violence to a person and damage to property[800].

3.5 Enforcement is also sometimes carried out through specialised police enforcement units that tackle online issues. For example, earlier this year the London Mayor's Office for Policing And Crime (MOPAC) launched a new Online Hate Crime Hub, which aims to improve the police response to online hate by gathering intelligence, improving understanding and testing new investigation methods[801].

3.6 On top of this enforcement, it is worth noting that the rules governing the internet and how online platforms operate are not static, they evolve to meet new and emerging challenges. In the last couple of years alone we've seen the introduction of new data protection laws, new codes of practice, and MOUs that deal with a wide range on online issues from misinformation to piracy. We have also seen regulators getting new powers, such as the BBFC's new remit for age-verification of online pornography.

3.7 Google is also working closely with the UK Government on a range of initiatives designed to boost online safety, such as the Digital Charter and the Internet Safety Strategy - both of which will help to hone and strengthen the existing framework.

[798] https://www.gov.uk/government/news/cma-secures-better-deal-for-cloud-storage-users
[799] https://www.asa.org.uk/advice-online/recognising-ads-advertisement-features.html
[800] https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media
[801] https://www.london.gov.uk/press-releases/mayoral/mayor-launches-unit-to-tackle-online-hate-crime

Internet Watch Foundation (IWF)

Google is a member of the IWF, who’s mission is the elimination of child sexual abuse imagery from the internet. For over 21 years, it has done this as a self-regulatory body in partnership with the industry.

The IWF works with international internet companies and collaborates with 48 hotlines in 42 countries, as well as with law enforcement partners globally, in order to provide a hotline for anyone to securely and anonymously report child sexual abuse imagery, and actively search for child sexual abuse images and videos on the internet.

The IWF provides hashes of (digitally fingerprinted) CSAI to the online industry to speed up the identification and removal of this content worldwide. This enables the internet industry to actively protect their customers and help victims of child sexual abuse. With funding from industry members, the IWF identified more than 80,000 instances of child sexual abuse imagery and analysed one webpage every four minutes, last year alone[802].

While challenges remain, robust analysis should underpin future initiatives

4.1 There are some that say the UK needs to change the ECD given the age of the directive and the changing nature of the internet. We would argue that as the online space evolves, the government can think about how social issues can be grappled with through new institutions or norms that build on top of the existing legal framework. This would avoid a wide range of unintended and harmful consequences of sweeping liability reforms which could include:

- Private businesses acting as censors: requiring platforms such as Google to review all user generated content before appearing on our platforms - and to remove content which it deemed inappropriate - this would require them to make legal or in some cases value judgements that are often more suitable and appropriate for the courts and public authorities, not individual commercial operators.

- Damage to freedom of speech: holding intermediaries liable for users’ actions and content can incentivise platforms to increase thresholds and filters in order to minimise risks of legal action against them. This risks severely chilling legitimate speech and narrowing the information and content available via the open web.

- Barriers to use: intermediaries would be required to introduce more onerous contractual terms on users who wish to contribute content to help minimise the risk of subsequent regulatory or legal action.

- Barriers to entry: forcing expensive content filtering technology onto start-ups and scale-ups would raise market entry barriers, potentially strengthening the position of only a few well-established players who can

[802] https://annualreport.iwf.org.uk/#awards_and_highlights

afford such tools. Equally, the expensive insurance premiums that start-ups would need to pay to shield them from liability claims, would divert funding away from innovation and would encourage a troubling "take down first, ask questions later/never" attitude to online content.

- Harming the UK's economic competitiveness: without protections for online intermediaries, creators, businesses, and consumers would not be able to use these powerful tools to reach and interact with new audiences, grow their businesses, or share their personal stories and viewpoints. This would have profound consequences for the entire online economy.

- Undermining collaboration: the existing legal framework is the foundation on which self-regulatory initiatives and industry collaboration are based.

Question 3: How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

Question 4: What role should users play in establishing and maintaining online community standards for content and behaviour?

5.1 Google recognises that we have a responsibility to ensure our platforms are used appropriately, that users have the tools and knowledge they need to make responsible choices online, and that they are able to report abuse which is acted upon swiftly. Google is committed to providing comprehensive and effective safety information, and we listen to our users and develop tools that are tailored to their needs.

5.2 We also make sure that once we enforce our policies and take action on any of our platforms, people have easy-to-use tools to challenge that decision, and have it overturned should a mistake have been made in the enforcement process. In some cases, we also give users the opportunity to make changes to their content so it no longer violates our guidelines.

Google's content policies are transparent and rigorously enforced

6.1 Google's wide range of products are governed by standards and content policies that reflect the variation in the nature of platforms and which set out clearly what we do and don't allow.

6.2 A variety of teams from Policy & Legal to User Experience & Privacy experts inform product content policy and provide advice to product leadership. These teams have a diverse range of backgrounds, from PhDs in privacy engineering to professional experience in civil society and technology governance. We also have Google employees with backgrounds in ethics. As we continuously evolve our policies, we frequently consult with outside experts including NGOs and academics, in addition to the expansive user testing that informs any changes and improvements we make to products and community guidelines.

6.3 For example, on YouTube, we maintain community guidelines that explain what kinds of content are not allowed and reflect the kind of community we hope to foster. The guidelines include:

- **Hate speech:** We don't allow content that promotes or condones violence against individuals or groups based on race or ethnic origin, religion, disability, gender, age, nationality, veteran status, or sexual orientation/gender identity, or whose primary purpose is inciting hatred on the basis of these core characteristics.

- **Threats**: Things like predatory behaviour, stalking, threats, harassment, intimidation, invading privacy, revealing other people's personal information and inciting others to commit violent acts are not allowed on the platform.

- **Depicting violence:** We do not allow violent or gory content that's primarily intended to be shocking, sensational, or disrespectful.

- **Inciting violence:** We explicitly prohibit terrorist recruitment and propaganda and other content posted with the purpose of inciting others to commit specific, serious violent acts.

- **Harmful or dangerous content**: Videos that encourage others to do things that might cause them to get badly hurt, especially children, are not allowed. Videos showing such harmful or dangerous acts may be age-restricted or removed depending on their severity. The promotion of illegal activities (bomb making, for example) is not allowed.

6.4 We also do not allow pornography on our major hosted platforms, including YouTube, Play, Google+ and Drive, or offer advertising on pornographic websites. All these guidelines are published online and made clear to all users with explanations available in many languages and formats: from videos to forums and policy centres.

Google’s users play a key role in enforcing standards on our platform

7.1 Google has rigorous reporting processes in place to flag and remove inappropriate content from our platforms, in which users play a key role. We want to act quickly when users inform us of content that might violate our policies, so we have pledged to continue the significant growth of our teams with the goal of bringing the total number of people across Google working on this to over 10,000 in 2018.

7.2 We work hard to ensure the decisions taken by these teams are fair and go through a rigorous quality assurance process. On YouTube for example, we have a formal review process whereby feedback on any incorrect decisions made by our reviewers is given directly to the reviewer who made the mistake and a root cause analysis is performed in order to learn and improve the reviewer’s accuracy.

7.3 As previously mentioned, this approach is complemented by state-of-the-art machine learning technology that assists us in managing content at scale on YouTube. When a user flags a video on YouTube, we use technology to triage based on content categories that are applied to videos when they are uploaded. YouTube is an important global platform for information and news, and our teams evaluate videos before taking action in order to protect content that has an educational, documentary, scientific or artistic purpose from being removed inadvertently.

7.4 To make our flagging process more efficient and encourage users to flag inappropriate, abusive or illegal content, we invite a small set of users who have particular expertise in identifying this type of content to join our Trusted Flagger Programme. Trusted Flagger membership gives users access to more advanced flagging tools as well as more granular feedback, making flagging more effective and efficient and helping us to take nuanced decisions and identify emerging areas of concern. The Home Office's Counter Terrorism Internet Referral Unit and the Internet Referral Unit at Europol also contribute to the programme alongside individual members.

Enforcement transparency

8.1 We also strive for transparency in the work we do to enforce the rules of the road. We recently published the first YouTube Community Guidelines Enforcement Report to show the progress we are making in removing violative content from our platforms, and we hope to update it regularly. The report is the first of its kind in the industry and includes public aggregate data about the flags we receive and the actions we take to remove videos and comments that violate our content policies and community guidelines, including data that is broken down by country.

8.2 Highlights from the report, reflecting data from October-December 2017, were:

- We removed over 8 million videos from YouTube during these months. The majority of these 8 million videos were mostly spam or people attempting to upload adult content - and represent a fraction of a percent of YouTube's total views during this time period.
- 6.7 million were first flagged for review by machines rather than humans.
- Of those 6.7 million videos, 76 percent were removed before they received a single view.

8.3 These statistics demonstrate the significant potential for machine learning to play a crucial role in identifying and removing problematic videos. Even so, human experts still play a key role in nuanced decisions about the line between – for instance – violent propaganda and religious or newsworthy speech.

8.4 Alongside the launch of our first global transparency report, we also recently launched a reporting history dashboard that each YouTube user can individually access to see the status of videos they've flagged to us for review against our Community Guidelines.

External oversight of community guidelines enforcement

9.1 Our work to enforce our community guidelines is overseen and scrutinised by a range of institutions. In September 2017, the European Commission published a

Communication encouraging online platforms to adopt a number of best practices to deal with illegal content, which it reinforced through a Recommendation issued in early 2018. Both outline guidelines and principles for how platforms should prevent, detect, remove and disable access to harmful content, whilst also highlighting the importance of shielding intermediaries from liability when they take voluntary proactive measures to remove illegal content from their platforms (the so-called "Good Samaritan" actions).

9.2 When it comes to hate speech more specifically, since May 2016, Facebook, Twitter, YouTube and Microsoft have committed to combating the spread of such content in Europe through the Code of Conduct. The third monitoring round shows that the companies are now increasingly fulfilling their commitment to remove the majority of illegal hate speech within 24 hours[803].

9.3 The European Commission also recently proposed measures to address concerns regarding disinformation, focused on the introduction an EU-wide code of practice, support for an independent network of fact-checkers, and a series of actions to stimulate quality journalism and promote media literacy. We will continue to engage with the Commission on the development of this code, building on our participation on the High Level Expert Group on disinformation.

9.4 On copyright, last year Google backed a code of practice from the Intellectual Property Office on the removal of infringing content from search engines, and we are working in partnership with other signatories such as the BPI to enforce it and tackle piracy online.

Question 5: what measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

Google has a duty to ensure our platforms are used safely and responsibly

10.1 In addition to enforcing our community guidelines and improving moderation and reporting functions, Google also dedicates significant resources to developing specialist products that help to protect users and enable them to choose how they interact with online content.

- Family Link helps parents stay in the loop while their children explore and enjoy their device. The goal is to enable kids to explore technology, while keeping parents in the loop on their child's digital activities and giving them the ability to make meaningful choices about their use of technology. Through Family Link, parents connect their phone to their child's phone or tablet, to set and tailor digital ground rules that work for their family, including:
    - Managing the apps their child can use - approving or blocking downloads.
    - Keeping an eye on screen time - seeing how much time their child

[803] http://europa.eu/rapid/press-release_IP-18-261_en.htm

spends on their favourite apps with weekly, monthly or daily activity reports, and setting daily screen time limits.

  - Setting device bedtimes - remotely locking their child's device when it's time for bed, or time to take a break.

- YouTube Kids provides a restricted version of YouTube for families with built in timers, no public comments, easy flagging, the option for parents to block videos or channels that they would prefer their child not to watch, and the option to turn search off for a more contained experience.

- On YouTube, content deemed inappropriate for younger audiences after review is "age-restricted," meaning it is only viewable by signed-in users who are 18 years of age and older who've clicked through a warning message. Parents can also turn on Restricted Mode so videos with mature content or that have been age-restricted will not show up in video search, related videos, playlists, shows or films.

- Google SafeSearch can be turned on with three clicks from the Google homepage and can be locked on, protected by a password, only removable by the account holder. While no filter is 100% accurate, SafeSearch helps people avoid content they may prefer not to see or would rather members of their family did not see.

Education campaigns are critical to boosting online safety, digital literacy and understanding

11.1 Google recently expanded our successful Be Internet Legends and Be Internet Citizens programmes, helping to provide more children than ever with the skills and knowledge they need to safely navigate the online world.

11.2 Be Internet Legends is an educational programme aimed at 7-11 year olds to help them become safe, confident explorers of the online world. Be Internet Citizens is aimed at 13-15 year olds and is designed to teach media literacy, critical thinking and digital citizenship; with the aim of encouraging young people to be positive voices online.

11.3 Through the programmes – both of which are accredited by the PSHE Association – Google will be visiting primary and secondary schools across the UK where we'll train 60,000 young people face-to-face through assemblies and workshops, and we aim to reach one million young people through our free training resources created for teachers and youth workers.

Protecting and enhancing freedom of expression

12.1 Freedom of expression and information are critical to Google and align with our mission to organise the world's information and make it universally accessible and useful. It is at the core of our community guidelines, and is at the forefront of our reviewers' minds when thinking about the kind of content we do and do not allow on our platforms.

12.2 Balanced protections and responsibilities for intermediaries under the ECD have been critical in supporting these aims and the free flow of information and expression on the internet. This has been recognised by a range of leading civil liberties groups. Independent human rights organisation, Article 19, has supported the role that intermediaries in facilitating connections and enhanced freedom of expression. European Digital Rights has also highlighted that the clarity of current liability rules supports freedom of information, thought and creation[804].

12.3 More recently, in response to Article 13 of the EU's proposal on copyright in the Digital Single Market, where new filtering requirements are debated, a range of influential organisations raised concerns on the impact they would have on fundamental rights[805].

12.4 The letter, signed by organisations including Human Rights Watch and the Open Rights Group, claimed the requirement to actively monitor users' content would contradict the 'no general obligation to monitor rules in the e-Commerce Directive, and 'violate the freedom of expression set out in Article 11 of the Charter of Fundamental Rights'. The letter also highlighted that the proposals 'would lead to excessive filtering and deletion of content and limit the freedom to impart information on the one hand, and the freedom to receive information on the other'.

Question 6: what information should online platforms provide to users about the use of their personal data?

Question 7: in what ways should online platforms be more transparent about their business practices - for example in their use of algorithms?

Google gives people transparency and control over their data

13.1 Google wants to support the proper functioning of the internet and people's trust in it. That means giving users transparency and control over the data that we use, and over the years we have developed many tools to help our users clearly understand what data we collect and how we secure it. For example:

- My Account is a single destination, unique to each Google user, which gives people transparency over the data we have and control over how it is used. Users can turn off personalised advertising, change interest preferences and, if they choose to, delete all of the information we have related to their account. In 2016, there were over 1.5 billion unique visitors to My Account.

- Privacy check-up is a procedure we proactively ask all Google account holders to go through at least once per year. It takes people to their privacy settings and asks them to manage the data they share, update the information they choose to make public, and adjust the types of adverts they would like Google to show them.

[804] https://edri.org/files/EDRi_ecommerceresponse_101105.pdf
[805] https://www.eff.org/files/2017/10/16/openletteroncopyrightdirective_final.pdf

- Ad settings allows people to amend, delete, or turn off completely personalised interest-based advertising from Google across Google services, as well as on websites and apps that we partner with. Ad settings preferences are cross-device, which means that you only need to make your preference choices on one device for them to be adhered to on any other devices you're signed into.

- On Android, our mobile operating system, we updated the permissions model for all apps in 2015 so that when users download an app they are asked for permission to allow the app to access certain information or features at the moment the app would like to access it. This empowers users to only give relevant data or use permissions to the apps that matter to them. For example a photo editing app would ask for permission to access the phone's camera at the moment you want to use the camera in the app.

13.2 More broadly, Google never sells its users' personal data. Nor do we let advertisers access users' personal data. Instead, we provide advertising that enable advertisers to target audiences with certain characteristics. We don't let advertisers use our services to directly identify who individuals are, and we do not allow ads to be targeted based on sensitive information such as race, sexual orientation, political affiliation or health.

Users have a strong understanding of Google's business

14.1 User trust is absolutely critical for us at Google, and we know one of the key ways to boost trust is to improve understanding. Overall, we believe that many people have a strong understanding about online platforms' business practices.

14.2 Ofcom's 2018 adults' media use and attitudes report found that more than half of adults (54%) are aware of how search engines are mainly funded, with the same research finding that more than seven in ten internet users (72%) say they are confident that they can manage who has access to their personal data online. Almost seven in ten (69%) say they are aware that companies use cookies to collect information, and almost six in ten (59%) know that companies collect information from social media accounts. Similar Ofcom research from 2017 also found that more children (12-15s) know how Google and YouTube are funded than how the BBC is funded.

14.3 But we know more can be done on this front so at Google, we use marketing campaigns and in-product communications channels to further educate our users on how our product work and how they can take full advantage of user choices and controls. Every day, nearly 20 million people around the globe visit My Account, our central hub that brings together all the different ways you can review your Google security, privacy and ad settings.

We work to ensure our products are transparent and understandable

15.1 Google is constantly striving to make the functioning of our products and services understandable to those who wish to know. We do this by explaining what the inputs and outputs are - giving a sense of what data is used, for what purposes - and a high-level description of how the algorithms work.

15.2 For Search, we provide a website describing How Search Works[806], over 600 videos on the Webmaster Help YouTube channel[807], and an interactive Search Console tool[808] for webmasters showing errors found on their sites and advising how to fix them, from diagnosing malware to reducing load time. The reason that this kind of transparency is helpful is that incentives align: if people try hard to get better rankings by making their sites easier to see on phones, that ends up helping their users.

15.3 When we consider modifications to Google Search, we have evaluators - real people who assess the quality of Google's search results - that provide us with feedback on the changes. Their ratings don't determine individual page rankings, but are used to help us gather data on the quality of our results and to help us identify areas where we need to improve. The guidelines that our raters follow - Search Quality Rater Guidelines - are available in full online, ensuring users and webmasters are able to scrutinise and understand how and why we make changes to our Search algorithms[809].

15.4 At the same time as boosting understanding of the inputs that go into algorithm design and how they help achieve desired outputs, we believe it is vital to promote public understanding about the purpose of algorithms and their responsible development and application. This extends to all forms of algorithms, including Artificial Intelligence (AI) and Machine Learning (ML).

15.5 However, we do not believe that complete transparency will always be helpful or productive, for example for algorithms. Pushing for 'full transparency' to reveal the raw code of a search engine would help people trying to game the system as well as conflicting with long-standing legal protections for trade secrets. Instead, we believe it is more valuable for users to understand the inputs that go into algorithm design and how they help achieve desired outputs.

15.6 We know from experience that bad actors will abuse our transparency in order to game our algorithms. Early in Google's history the founders published an academic paper on the PageRank algorithm that powered our initial search engine. Publishing the algorithm allowed malicious spammers to create giant clusters of fake sites that linked to each other and pay one another for links, which at that time led to higher Search rankings for the fake sites. We've since adjusted our algorithm to take this behavior into account, but this remains a constant battle. We already remove 1 billion spam results every day from spammers seeking to take traffic from more relevant, legitimate websites. The more bad actors know about the search algorithm, the harder it is to protect against such tampering, and the more difficult it is to give users the beneficial service that they require.

Question 8: what is the impact of the dominance of a small number of online platforms in certain online markets?

[806] https://www.google.com/search/howsearchworks/

[807] https://www.youtube.com/user/GoogleWebmasterHelp

[808] https://www.google.com/webmasters/tools/home?hl=en

[809] https://static.googleusercontent.com/media/www.google.com/en//insidesearch/howsearchworks/assets/searchqualityevaluatorguidelines.pdf

Online platforms benefit businesses and consumers

16.1 Internet platforms have reduced the costs of launching and scaling a business. Selling goods through online intermediaries - many of which are free - bypasses the need to invest in expensive technology and payments systems, lowering the amount of capital required to find new customers and enter new markets. This has helped to level the playing field between established businesses and SMEs, which now account for 85% of all new jobs across the EU[810].

16.2 By tackling these barriers to growth, online platforms have helped to create a diverse and vibrant digital economy. According to research from Copenhagen Economics, the total value of goods and services purchased through online intermediaries across the UK was worth €270 billion in 2015[811].

16.3 Online platforms have also helped to boost competition and lower prices for consumers. Intermediaries enable people to quickly access information and services outside of their immediate geographic area, opening up a more diverse range of products from a greater number of providers. This has helped consumers to make more informed decisions and lower the prices they are paying: online marketplaces have been estimated to enable lower prices for users of around 17% compared with retail stores.

16.4 Online search platforms have also been estimated to generate time savings worth €140 billion for European consumers in 2014, while free ad supported technologies such as search engines
and social networks generated a consumer surplus of €22 billion[812].

Google is a growth engine for the UK

17.1 Opening up the opportunity of digital technology for businesses and individuals is a key part of Google's work in the UK. From helping people to access information and acquire new skills and assisting businesses to launch their first website and trade online, we have opened up the Internet to the benefit of everyone..

17.2 Businesses use our tools like Search, AdWords (our pay per click search marketing program) and Analytics to attract consumers to their virtual and/or physical frontdoor. Our appstore, Google Play, allows UK-based developers to market their creations to users in over 190 countries.

17.3 Google's tools also help businesses to identify the most promising overseas markets by analysing search trends and volume for relevant terms and test their campaigns before making a large up-front investment. Given the costs of researching and preparing to enter a new market, this can help businesses to focus their resources.

[810] https://ec.europa.eu/growth/smes_en

[811] https://www.copenhageneconomics.com/dyn/resources/Publication/publicationPDF/2/342/1454501505/edima-online-intermediaries-eu-growth-engines.pdf

[812] https://www.copenhageneconomics.com/dyn/resources/Publication/publicationPDF/2/342/1454501505/edima-online-intermediaries-eu-growth-engines.pdf

17.4 A recent report from Deloitte found that for every £1 businesses in the UK spent on AdWords, they receive £3-£8 in profit[813]. Deloitte estimated that this created at least £11 billion in economic activity and supported over 200,000 jobs in 2014. Deloitte also found that publishers and content creators that use our AdSense advertising network - a tool for selling advertising space on a website like guardian.co.uk - generated at least £240 million in economic activity.

17.5 They found that YouTube Partners in the UK - creators who use YouTube to have their content reach a global audience while monetizing this work through advertising - generated at least £55 million in economic activity. YouTube also creates an export-first creative mindset.

17.6 Since 2015, through our Digital Garage we have also provided 250,000 people in the UK with free face-to-face training and visited more than 200 villages, towns and cities across the country. This forms part of our Grow with Google initiative – which aims to help everyone access the best of our training and tools – through which we have so far trained 5 million people in Europe, Middle East and Africa, helping to grow their skills, careers and businesses[814].

Question 9: What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

18.1 As the UK prepares for Brexit the digital sector should be recognised as a vital component of the wider economy. It is the second biggest industry in the UK, contributing over 16% of UK GDP, 10.1% of employment, 24% of all exports, and supporting three million jobs.

18.2 The digital economy will play an even greater role in the supporting the future economy; both for traditional industries like manufacturing and energy, but also in emerging ways including the use of data and technology in traditionally non-digital industries. 41% of digital tech jobs are now within industries that wouldn’t necessarily be associated with digital, such as education, health and financial services.

18.3 The UK government has played a key role in delivering the success of the digital economy. We encourage the government to continue to support this success by pursuing its industrial strategy, as well as a stable regulatory environment post Brexit, and recognising the importance of the tech sector to the wider economy.

18.4 We would welcome clarifications on how the application of important pieces of legislation, such as the ECD, will work post the transition period as this has a direct impact on investment decisions for companies and venture capital funds of all sizes. We would also encourage Government to consider setting up a Brexit digital taskforce that would promote investment and encourage start-ups and scale-ups.

18.5 Ensuring continued data adequacy with the GDPR so we and other UK organisations remain compliant and able to transfer data between the UK and EU and the rest of the world is also of critical importance. We are pleased to see the

[813] Deloitte (2015) Google’s Economic Impact, United Kingdom 2014

[814] https://grow.google/

Government's commitment to GDPR adequacy through the Data Protection Bill. However the complexity of achieving this should not be understated. We would thus ask that Government ensures this is a top priority during negotiations.

May 2018

Google UK, Facebook UK and Microsoft UK – oral evidence (QQ 174-182)

Transcript to be found under Facebook

Google UK – supplementary written evidence (IRN0121)

Thank you very much for the invitation to appear in front of the committee. As I mentioned during the session, this is a critical question for policymakers, and indeed for us as a company.

During Google's twenty years in operation, people's interactions with technology have significantly changed and evolved, which means the regulatory systems may need to change and evolve to meet new and emerging challenges, too. My colleagues and I are having active conversations on this issue. We are following the committee's work closely and will review your final report and any recommendations you may have.

You asked several follow up questions, and I'm happy to provide information on these.

We pay all taxes that we are legally required to pay in UK. This year we paid £49.3m in corporation tax. As with other companies based in the UK, we do not pay or calculate tax in relation to revenue. We recognise the fact that globalisation and digitalisation can pose challenges and we have said for several years that we are in support of reform at an international level. At the Budget, the government set a timetable for international reform. We will continue to work constructively with governments and the OECD on this issue.

You asked about the establishment of a new horizon scanning body to empower regulators. We believe it's important to consider carefully the issues which such a body could address. Ensuring that the internet is a safe and creative place for everyone, and that it can continue to support UK economic growth, is incredibly important to us. We all have a duty to support that, whether individual users, business or government. With technology and user habits evolving quickly, it is, of course, right that we look at how our practices keep pace, that includes looking at what is the best regulatory framework.

One of the reasons why this inquiry is so important is that, before we act, we need to identify the problems we're facing and be clear on what we're trying to achieve. This means looking at how people use the internet alongside how we deal with issues of freedom of speech and protecting people from harm. Given these are complex and fast-moving issues, we support progressing carefully on the basis of the evidence, looking at what we want to achieve and making sure that the policy is proportionate, keeps people safe, is future-proofed and avoids damaging unintended consequences, for example harming the UK's vibrant tech industry.

We do not want to pre-empt the inquiry and rule any particular course of action in or out at this stage. Our view is that we need to start from the basis of identifying the problems and then working out the best way to address them in a proportionate way, looking at the evidence.

We have worked diligently on delistings from Search under data protection law. Since the CJEU's 2014 decision in *Costeja*, we have delisted approximately 1,080,000 URLs under the procedure set forth by that ruling. We grant fast and effective responses to assert their rights in this respect. The delisting process under the EU's Right to be Forgotten takes into account the criteria set out by the CJEU when it first confirmed the existence of that right in 2014, as well as guidance from each country's regulators and courts. We publish statistics on these removals in our Transparency Report.[815]

Complaints about harms of a different nature need to be assessed under a different set of criteria, and as a result we have separate processes to address such requests. We publish statistics on these removals in separate sections of our Transparency Report.[816]

On the issues of mergers and public interest, competition authorities already have the tools to assess the impact of data when reviewing mergers and acquisitions. We have seen numerous examples of competition authorities requiring companies to behave in certain ways with respect to data, for example:

- The European Commission required Microsoft to make commitments regarding access to its APIs in order to approve its acquisition of LinkedIn.
- Gaz de France was forced to share customer data with competitors in order to increase competition in the French energy market.
- Google agreed with the US Department of Justice to continue to honour existing customer agreements to share data in its acquisition of travel data company, ITA Software.

Companies have been acquiring and utilising data for centuries, but recent technological developments have led to widespread availability of mobile devices, networking, cloud computing and databases that have made it easier than ever to organise and analyse data. This means that raw data is plentiful and value is only added through the processing of data.

On requiring an external body to approve our community standards, we understand that people want a clear view of how we are tackling problematic content. We recently started publishing quarterly global transparency reports which show the progress we are making on YouTube. This reporting was the first of its kind in the industry and includes aggregate data on flags we receive and the actions we take to remove videos and comments that violate our policies, including content that bullies or harasses.

We plan to refine our reporting systems and add additional data, including data on comments, speed of removal, and policy removal reasons. We have also introduced a Reporting History dashboard that each YouTube user can individually access to see the status of videos they’ve flagged to us for review against our Community Guidelines.

I hope this answers your questions. Do not hesitate to get in touch if we can help with anything else.

23 November 2018

[815] ‘Search removals under European privacy law’, *Transparency Report*, Google: https://transparencyreport.google.com/eu-privacy/overview [accessed 27/11/18].

[816] ‘Sharing data that sheds light on how the policies and actions of governments and corporations affect privacy, security and access to information’, *Transparency Report*, Google: https://transparencyreport.google.com/?hl=en_GB [accessed 27/11/18].

Clive Gringras - written evidence (IRN0110)

I am honoured that the Committee has called me to provide evidence. I regret that I was not able to attend in person; I hope that this written submission, nevertheless, provides the Committee with additional viewpoints on this important topic.

I am Clive Gringras, a Partner at the international law firm, CMS. Together with colleagues, I run its Technology sector. My first foray into the technology industry was in 1991, as a programmer of a computer game called Elite, written for the Acorn Archimedes, a great British computer whose RISC architecture still lives on in every ARM chip. Since then, I have been advising and commentating on the confluence between law and technology, most substantially with my book 'The Laws of the Internet' that was first published 21 years ago, now in its Fourth Edition.

My firm has a commitment to the technology sector. Our clients range from front-page household names to ones still operating out of the front room in a house. We have seventy-four offices advising on tech issues across forty-two countries. This give me the advantage of seeing the impact for the UK of turning the dial up, or down, on regulation for companies of all sizes. This submission, however, is the synthesis of my personal views on internet regulation.

Committee's questions on internet regulation

The Committee has stated that it is particularly interested in my opinion on whether I think it might be desirable to take a principles-based approach to internet regulation, and whether I think there should be a new regulatory body either to act as an ombudsman to deal with consumer complaints or simply to coordinate the work of existing regulators. Before addressing these head-on, I set out a general approach for considering questions such as these.

Focus on harmful use of the internet, not the technology itself

The Internet is a ubiquitous and neutral technology. It can be *used* by good people to do good, perhaps by using it as the medium to educate and entertain. And it can be *misused* by unwelcome individuals to cause harm, by publishing bullying comments or worse. If regulation is therefore needed to curtail harm and damage, it is not the "Internet" that might need regulating but rather the uses *of* the Internet and the behaviours *on* the Internet. But only where there are insufficient controls for those activities already.

This focus on activities *on* the internet rather than on the "internet" itself is a critical point. It's not merely semantics. The Committee will have two advantages by taking the approach of looking initially at the underlying mischief or concern. Advantage number one is that the approach will increase efficiency and advantage number two is that it will avoid definitional arbitrage. I explain these two advantages before moving onto my views on the Committee's questions to me.

Focus on efficient law-making

By looking at the underlying problem or concern first, say bullying or child protection, the Committee will be able to determine whether there is already common law or legislation that covers the underlying problem, even in part. For example, our legislative armory still contains the Protection of Children Act 1978. This Act has been adjusted to cater for new forms of harm such as pseudo-photographs of children, but this *foundational* statute was the basis for adjustments made in 1994, 2003, 2008 and 2009. In coding parlance, this is an "iterative" process. Such a process of looking at how existing legislation and law currently addresses the underlying harm or concern increases efficacy for all stakeholders. Parliament's time is not wasted "reinventing the wheel" when all that might be needed are small adjustments, or maybe nothing at all. Business does not need to get-up-to-speed on entirely new law. And our courts can continue to rely upon previous precedents and opinions.

Mitigate risks of definitional arbitrage

I stated above that there is a second reason why this Committee should focus on the underlying issue, and not be tempted to look at the medium being misused by the bad actor: definitional arbitrage. If one creates laws that are directed to harm perpetrated over the Internet, how is that same behavior treated when perpetrated *off* the Internet? If that offline activity is already regulated, why was there a need to create a whole new law for the Internet? A simple and uncontroversial adjustment is all that's needed. If the offline equivalent is not already regulated but regulation of the online harm called for, why is the offline harm being dealt with more leniently than the online one? Differentiating the treatment of a harmful activity based on the type of technology or medium used creates an incentive for debates over whether the bad act took place on the Internet or not. Businesses and defendants might spend time arguing that their activity *definitionally* falls on the lenient side of the regulation. Hurt citizens will, in contrast, spend their time arguing that the harm originates from the stricter side of the law. All this will lead to lawyers and courts needing to figure out what the draftsperson meant.

If citizens need more protection – *all* citizens must be protected, not merely those unlucky enough to see their rights abused online. We saw this when the 1984 Data Protection Act wrongly protected only digital, not offline filing systems. It should instead have focused on privacy rights in general and not on what medium the bad actor abused to cause the harm. It was no consolation to victims that their privacy rights were breached on paper rather than on a screen.

Avoid Internet-specific regulation

It should follow from the early part of this submission that I do not believe that there should be an "internet regulator" – not because there are no legitimate societal concerns over certain behaviours and activities conducted over the internet. There clearly are concerns. There should be no "internet regulator" because if there is a concern, the existing legislative and regulatory framework should be utilised. For example, when Parliament determined that there needed to be stronger consumer protection controls over "digital content" in the Consumer Rights Act 2015, it was correct they gave enforcement of that to the usual consumer enforcement bodies such as the CMA and Trading Standards. Similarly, where there is fraud being perpetrated over the Internet, that should fall on the desk of the FCA and others charged with policing and regulating financial services.

A follow-on question might then be, "so what should be done when it *is* evident that existing frameworks are failing?"

Sadly, even where the strongest criminal laws are in place, there are still those who will commit offences. That people break the law despite a clear prohibition in a statute does not necessarily mean that the law – the text of the legislation – is wanting. It might mean that the police require greater funding to prioritise investigation and better resources to track down perpetrators. It might even mean that our prosecution service is prioritising other seemingly more-pressing matters. It possibly might even mean that our courts require additional training on certain matters. But just because bad people do bad things does not mean that there is a need for new legislation; it might mean that the legislation requires more support from the rest of the enforcement community.

Even where there is a clear gap in the legislative framework, the first step should be to think internationally and not only parochially. Legislators should investigate and consider the international reaction to the same activity. Not because we in the United Kingdom have to follow but to ensure that we are not creating legislation that will not apply to the foreign actors and to ensure we are not creating legislation that might conflict with the laws of other countries. In addition, any new law or approach to activity on the internet might have the unintended consequence of scaring investment away from innovation and away from the UK to more indulgent overseas regimes.

If a proper investigation of overseas laws and regulations has been completed and reveals a clear and justified need for greater oversight in our country, what form is appropriate? Because of technology's velocity and the depth of penetration into all aspects of society, I believe that co-regulation or self-regulation is the optimal approach. This is not because I believe it to less onerous or less impactful. It's because by bringing together the collective brains from the industry, from across the world, to solve and deal with an issue the costs of the approach stay off the public purse and, society wins with a quick, flexible and cost-effective solution.

Few would disagree that child abuse, and child sexual abuse content, is one of the most important areas to curtail and rid from our society. And one of the best examples of how this country protects children from being abused is the astonishing work done by the Internet Watch Foundation and its evidence before this Committee is compelling. When I first wrote about this organisation in my book in early 1997, 18% of this awful content was hosted in the United Kingdom. Now it's less than 0.1%. Last year the IWF worked to remove over fifty-five thousand websites. It's not just an example of self-regulation working it's an example of something which is over twenty-years old, and still working. There are other self and co-regulatory success stories such as the way in which search engines and rightsholders now have a voluntary code on intellectual property and, from the latest data from the Intellectual Property Office, have hit their targets.

What is key is to work backwards from the harm that you are seeking to prevent and then carefully to consider whether it's occurring because, unfortunately, bad things happen even with strong legislation – so perhaps enforcement needs to be stepped up – or whether it's occurring because the underlying legislation is inadequate.

Effect of leaving the EU

Having just discussed the need for international visibility, it natural for this submission to address the impact of Brexit on this area.

Our entry into the Union almost coincided with the founding of Microsoft. The Maastricht Treaty came into force seven months before the founding of Amazon, and Facebook was founded just weeks before the 2004 expansion of the EU. Our Parliament's experience of the internet's impact has only been whilst the UK has been in the EU. Much EU legislation in this area is well-considered, world-class and future-proof. For example, the EU's Electronic Commerce Directive, and many other laws like it, strike the correct balance between protecting society from the misuse of the Internet without jeopardising the enormous societal, cultural and educational benefits that this technology offers. Respected lawmakers on every continent have emulated the Electronic Commerce Directive's notice and takedown-type provisions rather than imposing general duties on Internet companies, for example. And that is why I am massively supportive of Committees like this one – seeking to build new understanding of the area – so that the UK will be self-sufficient when law-making whilst being highly cognisant of the international implications of any decisions made.

July 2018

The *Guardian*, The *Times* and *Wired UK* – oral evidence (QQ 152-160)

Tuesday 23 October 2018

Watch the meeting

Members present: Lord Gilbert of Panteg (Chairman); Lord Allen of Kensington; Baroness Benjamin; Baroness Bonham-Carter of Yarnbury; Baroness Chisholm of Owlpen; Viscount Colville of Culross; Lord Goodlad; Lord Gordon of Strathblane; Baroness Kidron; Baroness McIntosh of Hudnall; Baroness Quin.

Evidence Session No. 18 Heard in Public Questions 152 - 160

Examination of Witnesses

Mark Bridge, Technology Correspondent, The *Times*; Matt Reynolds, Staff Writer, *Wired UK*; Alex Hern, Technology Reporter, The *Guardian*.

Q152 **The Chairman:** Can I welcome our witnesses to today's session of the House of Lords Communications Committee, part of our inquiry into internet regulation? Our witnesses today are experts in the field, and reporters and journalists in the field of technology. We are very grateful to you, gentlemen, for joining us. I know as journalists you are more familiar with asking rather than answering questions, so it is good of you to come along here and share your experience and indeed your expertise with the Committee. Our witnesses are Mark Bridge, who is technology correspondent at the *Times*; Matt Reynolds, who writes for *Wired UK*; and Alex Hern, who is technology reporter for the *Guardian*. It is good of you to be here. We will be recording today's session. It will be broadcast online and a transcript will be made.

Perhaps I can open by asking you to say a few words about your background and any top-line observations that you might have. In doing so, perhaps you will address our first question area: what do you think are the most serious risks to individuals and society that have been enabled, facilitated or worsened by the internet? How, in your experience, do Government and Governments step up to managing those risks?

Mark Bridge: I am technology correspondent at the *Times*. I have done that for about two years. I have been at the *Times* for 10 years, working on other beats. We write quite a lot on these issues, in terms of online harms, issues around regulation and social media issues generally.

In terms of the most serious risks, there are several that stand out. There is the terrorism issue, as in the fact that the internet and social media have allowed terrorists to share their propaganda, to recruit people, radicalise them and incite terror attacks. Almost all of the terrorists behind recent European terror attacks have seen this kind of material. There are also sexual predators who have used the net extensively. Europol had recent figures showing that the amount of this kind of material has proliferated despite all the efforts to crack down on that. Of course, there is misinformation generally and attempts to sow discord in the West and undermine our democracy. There are lots of other potential harms but those are the ones that stand out.

In terms of Governments and how they can address that, it has been a free-for-all until the last couple of years. Not much has been done until a spotlight has been put on to these things and there has been relentless pressure on these companies. It has been a real effort to get them to do anything but the pressure is starting to achieve some results. There are lots of questions about how you regulate effectively. I do not know if there are specific questions.

The Chairman: We will move on to some more specific areas. Thank you, Mr Bridge.

Alex Hern: I have been a technology reporter at the *Guardian* for five years now. Before that, I covered economics at the *New Statesman*. I do not disagree with anything Mark has said. There are just a few other areas that I would add. For individuals, a really important risk to take into account is effectively the risk to mental health. The internet and modern communication technologies are radically different from what existed before them and people have a radically different relationship to them. Effectively, the internet flattens relationships. You feel very close to a lot of people. That is broadly new. We as humans are not used to feeling close to 1,000 or 5,000 people. That alone can be extremely difficult and can affect people who are susceptible to mental illness in bad ways.

Also, at heightened moments it can obviously have a negative effect. The stories you hear about online Twitter mobs, for instance, are quite frequently people saying things that would be sort of normal and okay if four or five people said them to you, but we are not able to deal with 10,000 people hurling quite vicious abuse at us all the time, even if, frankly, if three or four people said that to us, we might go, "Hands up. You know what? That was a silly thing to have said". We are not used to, as humans, having to deal with these numbers.

That same problem affects young people on Instagram feeling like they have a very close personal relationship with 500 influencers. They might think they are close personal friends with 500 beautiful people who work out every day and have wonderful sponsorships—you can see where I am going. The way that you react to these people is different from anything before in society.

Similarly, when it comes to risks to society rather than the individual, everything Mark said is true; but there are also broader problems with society's ability to even understand and deal with some of the changes that have been wrought. We can talk, using the language we have built up over the last century, of the problems that encrypted messages on WhatsApp pose to policing. We know our society. Our intelligence agencies know how to discuss the problem of people having communications that they do not have access to. We do not really know how to talk and we do not have a language to discuss in the same way, with the same broad participation, the problems of rapid loss of trust in conventional media sources and problems of the flattening and widening of who is trusted. We do not know how to analyse that and so there are clearly risks there. Whether or not it is actually a downside, I do not know. It may prove in the long run that a world in which 10,000 YouTubers provide the bulk of news reporting analysis for the UK is a better world with a better media climate, but it is a risk. That is the sort of risk that is hard to elaborate on without the sort of research that I hope this Committee will do.

Matt Reynolds: I am a reporter for *Wired UK*. Before that, I covered a similar beat at *New Scientist*. I get the pleasure of going last so all the clever stuff has been said, but I definitely echo what Alex and Mark were saying, especially Alex's point on thinking about the flattening of information hierarchies. That seems such an undercurrent to lots of the stuff that is going on today. It is that flattening of hierarchies combined with the fact that you have a very small number of platforms, thinking about Google, Facebook and Twitter. In particular if you think about misinformation, or information more generally, those two combinations seem to be a vastly underlying factor. If you are looking at things like Russian interference in the US in 2016, far-right extremism in the UK, unrest in India on WhatsApp or ethnic cleansing in Myanmar, it seems to me that this is a very obvious undercurrent.

Perhaps that is one side effect of the clustering of so much power and so much of our everyday time in the hands of this very small number of companies. Think how many times today you interacted with Google, Facebook, Apple or whatever. The narrowing of the number of touchpoints that we have represents, like Alex said, a really huge opportunity. In terms of what it enables, it is certainly nothing like we have had before, so it is really exciting, but it seems to me that a lot of the risks stem from that centralisation of power and time spent.

Q153 **Baroness Benjamin:** From what you have all been describing and what is actually happening, it seems that, in terms of where we are at this point in time, you might say that progress does not always take us forward, because of the everyday events that you described and the behaviour that has been happening. Can I ask each of you: what are the strengths and weaknesses of the current regulatory framework of the internet, which now, as you said, is embedded as part of our lives and our society? How do you feel it can be improved?

Mark Bridge: There is not really a regulatory framework for the internet. It is very hard to achieve one, given its global nature. There are certain areas that are regulated. There are attempts to get the companies to self-regulate, which have achieved certain things. The companies would argue that there are advantages to self-regulation. Very clearly there is a lot of stuff that has been highlighted again and again, and not much has changed or nothing has changed. It is being looked at but age verification, for example, is a huge deal, in that the sites will say we do not have under-13s on our platforms. Ofcom showed that about 23% of 11 and 12 year-olds are in fact on these social media sites that they should not be on. That should be something that can be dealt with fairly easily. It has not been.

Baroness Benjamin: By whom?

Mark Bridge: The Government need to work with companies to develop technical solutions but that should be something that can be done. There should be a way to check the age and identity of those on your service.

Baroness Benjamin: Who should check it?

***Mark Bridge*:** The platforms should, but there should be some standard, presumably, that they would work to.

Baroness Benjamin: You think it should not be a regulatory body; the platforms themselves should check this.

Mark Bridge: Yes. There could be something akin to what is coming in with pornography, for example.

Baroness Benjamin: I see what you mean.

Mark Bridge: Children on these platforms are exposed to so much that is potentially harmful. There was recently a stat on the percentage of children who are targeted by predators; I think it was from an FOI request. Approximately 75% of them had been targeted via the main platforms—things like Facebook, Snapchat and possibly Twitter.

Baroness Benjamin: What you are saying is the BBFC is going to be looking at porn but it should be looking at other things.

Mark Bridge: I do not know whether it should be the BBFC but I think there should be a solution along those lines to keep kids off these platforms. The companies themselves acknowledge that children should not be on these platforms. Again, that can be used with apps that, in theory, are not suitable for 13 year-olds or whatever it is, but six year-olds are downloading them, using them and being exposed to gambling and all sorts of sexual content, whatever it is.

Alex Hern: The strengths and the weaknesses of the internet, when it comes to regulation and when it comes to the internet itself, are the same thing. The strength of the internet is that for most of its history no one has needed to ask for permission to do anything on it and almost anything they can conceive of they can build. That has allowed an incredible flourishing of innovation worldwide. That is not a strength to be dismissed. It is also quite clearly the weakness. The weakness of the internet is that anyone can do anything on it without asking permission. That allows all of the misuses of it that we have seen and heard about so far.

When it comes to obvious areas for improvement, the things I would suggest the Committee looks to are the areas of the internet where that upside—the ability of innovation to flourish—sort of no longer exists. That is because a significant chunk of the internet is actually now quite heavily controlled by a few small power-brokers, which are the same four or five companies that we will hear about for the rest of this session. It is no longer the case that you can do anything without asking permission on a site like Facebook or on a platform like YouTube. These are now fairly centrally controlled. Although Facebook likes to talk about the organic growth that happens on its site, if you actually post something to Facebook, the site will very quickly come back and ask you for money and tell you how many more people you can reach if you pay it. It is acting like a conventional power-broker of the sort that the media industry is used to and that we understand how to deal with, to a certain extent. I would suggest that that also slightly nullifies the upside of a lack of regulation. If it is no longer the case that anyone can do anything, then it is also no longer the case that that light-touch regulation is having much of an upside.

On the specific points that Mark has already brought up relating to young people online, there is a second area where there is again this symmetrical strength and weakness, and that is anonymity online. Again, one of the upsides of anonymity on the internet—the assumption that you do not have to prove you are who you are—is that people can socially and culturally reinvent themselves. They can have communications with people who may not want to talk to them if they knew who they were. They can, for instance, reach out to journalists without revealing their identities, to leak information or just to provide expert insight. That is an upside; and again, it comes with its symmetrical downside. I do not think it is easy. I do not think you can simply remove anonymity from everyone, which is what age restrictions would entail because you obviously cannot ask only young people to prove they are who they are; you have to ask everyone or you ask no one. There is a strong downside to that.

Again, the places I would say it fits most obviously with the current state of the internet are the places where that anonymity has already been removed. Facebook enforces a real-name policy. If people have names that the site moderators do not recognise as real, it asks them to upload identification—typically state identification. It has already done that in some unpleasantly heavy-handed ways. Native Americans in America have reported being disproportionately targeted by this because traditional native American names sound, to someone who has not heard them, like they might be a joke name. A lack of cultural awareness has led to unpleasant enforcement.

Similarly, people with famous names, frankly, have reported being unfairly targeted. If your name is Mark Zuckerberg and you are not the Mark Zuckerberg, I cannot imagine you get to use Facebook without providing some ID. I do not think there is as much of a downside on those platforms to removing that presumption of anonymity as there would be if we tried to apply the same rule to the internet at large. It is that symmetry. The benefits of light-touch regulation are quite broad and quite intrinsic to the internet, and I would ask the Committee to be careful when considering whether to remove them and to look at whether or not they are in practice still there in the first place.

Matt Reynolds: I would agree with a lot of that. The light-touch regulation of the internet is essentially what has shaped it as an incredibly useful resource now. Essentially it means that what we have ended up with is a fractured, self-regulatory environment where what passes as hate speech on Facebook is not the same as what passes as hate speech on Twitter, and the same with YouTube. This is really problematic. At the moment you get a very ad hoc approach to dealing with any of these issues. Take the banning of Alex Jones. I think Spotify removed a podcast, then you see it in Twitter and then you see it in Facebook. Actually, if he was in violation of all of their terms of services or community guidelines at the same time, there should have never been any question that you would have this conga line, if you like, of banning.

It suggests to me that there is a space for at least some kind of alignment between these. If this is where we have our public conversations, if this is where we think about it, we need to be thinking about what kind of standards we can enforce and what is expected. At the minute, it is very responsive to press and media coverage but it does not have any coherent outline. I see that when Germany basically forced Facebook and social media to do more to combat hate speech, Human Rights Watch basically attacked that as a worry for overt censorship. I really appreciate that it is a very difficult thing but some sense of alignment on that is a good idea.

To your point on thinking about whether you offload this responsibility on to a regulator or whether you ask the platforms to self-regulate, we have to expect that at this scale that we are talking about, with the scale that these platforms are, they have to build self-regulation into their very scale. I do not accept the argument that you get to have this reach of 2.2 billion people and then say, "We forgot how to check out like we did before". It should be a requirement of building these platforms and building that reach that you have the ability to be on top of that.

"Self-regulation" is the wrong term; self-moderation that is overseen by a regulator makes a lot of sense to me. We should not offload the responsibility of catching it to the press or to whoever, but we should be realistic about who is capable of keeping that eye out. It seems to me that it is going to be the platforms that built these things in the first place.

Baroness Benjamin: What about current regulatory bodies such as the ICO? Do you think that they are effective and properly resourced in regulating the internet and could solve the problems that we are facing?

Matt Reynolds: My sense is no, insofar as thinking about the ICO specifically in terms of the amount of money they are able to leverage for fines. It is hard to see, because it very early days in terms of enforcing GDPR, whether companies respond to things like that. I do not have an awful lot of faith that they are well enough resourced or that their remit is outlined clearly enough or that their ability to effect change in those organisations is realised or felt enough.

It feels to me that possibly—and this is no surprise because of the headlines it has gathered—the EU's competition authority has probably done the most in making tech authorities listen. This is probably for a couple of reasons: first, just by virtue of the amounts they can leverage and force; secondly, if you are Google, you are thinking about what affects a market of 300 million people and how you can shape your service so it aligns with those. This is a point we will get on to, but the weight of having policy that aligns with a broader environment like the EU makes an awful lot of sense. It gives it a lot of persuasive power.

I am not totally convinced. Aside from the ICO, in the UK it is so fragmented. Where was the Advertising Standards Authority when we were talking about Facebook ads? Consistently, existing bodies have not stepped up or seen that their remit extends to the online world, if you want, which is literally just our real world. So far, there have been quite a lot of failings in that respect.

Baroness Benjamin: Do you think there should be perhaps a global regulatory framework body that gets it all together?

Matt Reynolds: Do you mean internationally?

Baroness Benjamin: Yes. At the moment, you are saying it is all fragmented, people think it is somebody else's problem and we are not really having that joined-up, holistic policy that we should have, because, as I said, we are progressing and progress does not always take us forward. How much further are we going to progress without literally making sure that we have a framework that is looking after the interests of people, especially our children?

Matt Reynolds: The worry with a global authority is that you think that there are a billion people living in China who have a very different idea of privacy than we do. There are so many people in America that again have a very different idea of privacy and rights than we do. There is a pay-off, right? If you are Google, a site of 300 million or a consumer pool of 300 million is sizable; it would influence your policy and it would make you think.

I am not completely against the idea but my worry is these voices in Silicon Valley are so influential that when you bring in factors like China, perhaps finding this perfect point that everyone works towards just might not exist. What can we do in the UK? We can probably defend the things that we think are right for the internet, and we should not be that afraid to try to enforce that as best as we can and say that if the global standard does not step up to what we think is appropriate and the type of things that we want to see, that is something you have to pull in line with and that we do not have to step back towards. That is probably impractical but I would be a bit worried about the kind of influence a global body would have.

Q154 **Lord Gordon of Strathblane:** I have a further point. It is almost inevitable that however well sourced regulators might be, either present ones or possible future ones, at some point they are going to recommend to Government that somebody legislates to do something. Do you think Government, as we have it at the moment, and Parliament are properly structured to cope with something as fast-moving as the internet? If, as I suspect, you think it is not, how would you recommend it improves?

Alex Hern: The fast-moving nature of the internet is not as antithetical to regulation as it might seem. There are a lot of regulations and a lot of proposals that can be phrased in human-readable language, rather than technical language. I agree it would not be appropriate to pass legislation saying that, for instance, if something has more than 5,000 retweets it should be deemed that the platform should pay attention to it because it has been seen by a lot of people. That sort of thing would never work but with the Advertising Standards Authority, for instance, it is not clear to me that you need to write technical language into their code of practice for their remit to be extended to the internet. They judge advertisements based on non-technical standards: accuracy, truth. Those have not been changed that much by the internet. I do not quite understand why something being online means that the legislation has to be written in such a way that it cannot be future-proofed.

Q155 **Baroness McIntosh of Hudnall:** I want to ask any of you who want to pick it up about other regimes. You made the point, Mr Reynolds, that we ought to be looking at what we can achieve here given that attempting some kind of global reach is probably beyond any particular parliamentary competence. What is your view of, for example, what has happened in Germany, where they have politically taken a much tougher line on certain kinds of regulation than, for example, we yet have? Do you think that has been a move in the right direction, or do you think it has had unintended consequences in terms of free speech or any of the other things it might have impacted on?

Matt Reynolds: It is a really difficult question, which is no surprise. I know this sounds maybe like an evasive answer but it comes down to the fact that if the German Parliament is tasked with enforcing policy that it believes is right to protect people in Germany and is right for that, I do not necessarily see that that would be an example that we would want to follow just because they could and because they have. It underlines the idea that we should be having this public debate. An organisation like Doteveryone, which I presume spoke to you as part of this process, is really good for having that debate and deciding what we think is acceptable and what should be legislated for and what should not. There is a lot of work assessing where we are at with that conversation that we need to come to before we think about how we can put in place laws that align with this.

I would also add to what Alex just said. If you think perhaps about our free speech law or our speech laws more generally, I am interested to know what specifically about them being online means we have to update or do something new. We should be thinking, "If these are the standards that we apply to public speech, public broadcasting or that type of thing, might we think usefully how we apply it online?" I do not think we are coming completely from scratch, not saying, "Should hate speech be on the internet?" so much as, "What is acceptable to come across in your daily life?" Perhaps if we think about that, we have a body of legislation, a body of evidence and clever people who are thinking about this, which we can leverage more easily.

Baroness McIntosh of Hudnall: You might think that the difficulty there is actually in implementing and sanctioning. The basic principles may be right but applying them in the world of digital technology is perhaps slightly more difficult, would you agree?

Matt Reynolds: I agree that it is more difficult. To slightly push back on that, I completely agree that it is difficult and the scale makes it difficult, but it being difficult should not be an excuse. When we are talking about the scale and difficulty, we are also talking about companies that have vast resources, are hugely influential and are in a position where, frankly, they should be stepping up to it and having this conversation. A factory manufacturer does not scale up and say, "It is unsafe. We are moving really fast. We are trying to get to everyone and do loads of products". We need to start, in our terminology and how we think about this, to demand a lot more and expect a lot more, because they are huge, they are influential and they are already reaping the benefits of scale. It is time to think about how you apply the responsibilities of that. Difficulty cannot be an excuse, although I completely appreciate that it is difficult.

Q156 **Lord Goodlad:** You have already covered some of this in your discussion following Baroness Benjamin's original question, but could I ask how effective you think platforms are in moderating content so as to protect users from harmful content and online abuse? Secondly, what measures should, and indeed could, be instituted by platforms to improve their content moderation and their complaints procedures?

Mark Bridge: If you are talking about sites like YouTube and Facebook, they are increasingly successful in using algorithms, which are quite crude, to identify some of the most egregious content. They are good at picking up some of the jihadi material and a lot of the paedophile stuff. I am talking about on the big, main social media platforms. What tends to happen is it gets pushed on to smaller platforms and smaller websites, to some extent. We wrote this weekend on a report by some analysts in the States, which showed that jihadi material was being pushed off YouTube but a lot of it was appearing on Google Drive and Google Photos, for example.

They have the AI technology to make some progress on this but they tend to rely on artificial intelligence, on the one hand, and human moderators looking at flagged content, on the other hand. That is content that has been flagged by users or, in the case of Google, trusted flaggers, which are organisations they work with. My sense is that the number of humans involved in this is still far too low given the enormous resources we have spoken about, and the degree to which they will proactively look for any of this stuff is, again, fairly small.

I have one quick point on that report I mentioned that we covered, showing stuff was being pushed from, say, YouTube on to these smaller platforms. In that report, they made the point that the resources of your Googles and Facebooks should be used to back up the efforts of the smaller companies that do not have the same kinds of resources. They have not only the financial resources but the technical ability to assist a lot of those smaller companies that need to be involved in this as well.

The Chairman: Mr Hern, is the failure to resource human moderating a key part of the problem?

Alex Hern: It is, yes. It is slightly unbelievable that any platform with users measured in the billions can count its human moderators in the thousands. That seems to be a scale error. It is not the case that you need someone to read every piece of content that goes up. I do not believe that is what anyone is requesting but, none the less, more people helps. More people allows, first, quicker turnaround times, which is the obvious request for issues like child abuse imagery and terrorist content. More people also allows longer, more nuanced, more considered review, which is of course a symmetrical problem. For everything that gets left up wrongly, there are things that get taken down wrongly as well.

I am sure all three of us have had situations where we have reported both of those things to the companies, only to find that miraculously when a journalist is spotted, they reverse their decision. One goal for moderation should be that happening less often. It is odd that journalists, without any of the in-house tools to mechanically search through these things—a journalist just uses the public entry points—can so consistently find examples where the policies have been implemented wrongly, either too strongly or not strongly enough.

Beyond simple resourcing, an almost larger issue is transparency. The problem is that Facebook has published vague versions of how they apply their rules. Most of the other companies have not even published those. It is still very unclear how any of this actually happens. Without that, it is hard from the outside to really recommend anything. We do not know. They talk about themselves as though they are operating miniature states with judges and juries but, if they are, it is sham justice.

Matt Reynolds: I completely agree with all that. To add from my own experience of reporting, I did a story around some really nasty far-right pages on Facebook that had a reach of millions of people in the UK. Obviously I spoke about this to Facebook. They were not taken down because they did not apparently violate the community standards, even though they were talking about siphoning funds to militia groups. It was very, very bizarre. A couple of months later I then found out that they had been taken down. I got back to Facebook. It was very hard to get an answer from Facebook as to why this happened, but the answer was that a post had violated their terms. We are talking about a network of 12 pages with millions of people.

Like Alex was saying, there is not this consistency. That is a big problem. There is not this transparency. Furthermore, is not applied uniformly when it comes to sites of that scale. Especially when it comes to sites like Facebook, you have to remember that groups' reach and success on these networks are how they make their money, right? It is a problem. If these rules are not enforced uniformly and scale comes into it, you start to wonder, "Well, it should not be a factor who commits the crime or violates the hate speech". In my experience, it seems to be that those are not uniformly applied. It makes my job quite difficult, to be honest. It worries me slightly.

Baroness Quin: I am struck with what Mr Hern was saying about them not publishing their own rules. Are there ways in which they could be obliged to publish their rules, either through the EU, if that is big enough to do it, or through consumer demand? Lots of petitions get organised for all kinds of things. Is it conceivable that one could have a petition of angry consumers saying that they wanted to know exactly what these rules were?

Alex Hern: That is what I was going to say. This takes it back to one potentially fruitful avenue of regulation. If a regulator's job is not to sit on the outside and attempt to moderate these companies themselves, which would be horrendously expensive and very hard to do externally, a good avenue to explore would be a regulator whose job it is to ensure that these rules are applied consistently and fairly. Obviously one part of setting up such a regulator would be that the regulator would have to demand to know what the rules actually are.

It does feel that a regulator whose job it is to—in the German style—demand that hate speech be taken down in 24 hours or they will issue swingeing fines, is obviously going to result in an overcorrection; it is going to result in what has reportedly been happening in Germany so far, where anything that has the slightest whiff of hate speech is taken down. I believe that in the German public sphere that is not seen as that bad a thing. Here we have less of a hard-and-fast desire to fully censor all potential hate speech from society. We are a more open society in that regard.

If rather than that we have a rule that says, "Your rules about hate speech must be clear, open to your users, applied consistently and applied through a moderation process that is worth its salt", then you start coming to it being actually quite fair to fine for breaches of that. If you find out that Facebook left up some hate speech because it was from a user that had a million subscribers and contributed quite a lot of video that generated ad revenue, that is the sort of thing that a regulator should be clamping down on. It is a fruitful avenue.

Q157 **Viscount Colville of Culross:** I would like to declare an interest as a series producer providing content for the Smithsonian Channel and also for CNN. I would like to ask you about fake news and your views on the significance of fake news in threatening the trust the public have in online media. What is to be done about it? Alex, you have just talked about transparency. Matt, in your *Wired* article on the fake news interim report from the House of Commons, you said that the report was an "indictment of technology companies' opacity". Should we get any future regulator to enforce transparency so we know where the sourcing is and we know where the users are? Can you tell me about that?

Matt Reynolds: I certainly think that in terms of the sourcing, yes. What fake news or misinformation has done does not just affect online media but more broadly it has played into this quite cynical distrust of authority or news more generally. I would say that at the very least it makes an awful lot of sense to flag up the source of where information is coming from. Although, to be honest, I wonder whether that would necessarily solve anything. If the source is Tommy Robinson and that source does not use facts or that source is erroneous in their reporting, does it matter if it was Tommy Robinson? In fact, it is the virtue of the brand of Tommy Robinson that attracts people and not their reporting credentials, if you like.

Sorry, I realise that I am not offering a solution, but I think that the problem is that when you say, "We need to factor in all that stuff", I completely agree, as a value judgment for what people say news should be. The big problem with Facebook is there is news, not news and all these blurs. It is almost like you have to make a decision: "Is this thing presenting itself as news? Then it has to meet these standards. Then, should it be somewhere else?" I cannot see exactly what you would have.

It is a good idea to have more transparency, and there should be more vetting and more openness. It is a really complex problem that would not necessarily just be solved by saying where it comes from. We need to decide what information is useful and what context is useful to provide. Do we talk about who is funding it? Do we say that they have been brought up for this violation before? There is all this stuff. Yes, there are lots of questions before we get there.

Alex Hern: Fake news and misinformation online is an extremely difficult topic. It is hard to even define the terms of the debate. When fake news first started being used as a descriptive term it was referring to sites that published stories, created out of a whole cloth, to gain revenue from adverts that were run on them, and were shaped largely to talk about American politics because that was where the most readers and the most obvious readers for shock news at the time came from. That is, as a category, quite easy to deal with because, for one, the ad networks—networks such as Google, who effectively fund these sites—do not really want to fund these sites and did in practice begin pulling adverts from them quite rapidly. Again, in terms of what we were talking about earlier with older regulations kind of still working in the internet age, much of what these places publish is libellous and defamatory, and they do not hold up very long if anyone wanted to sue them. They also have a short shelf-life.

The broader problem is the lack of public trust that they have engendered. In short, the broader problem of fake news is that now people call real news fake news. I do not think there is an easy way to solve that. I may sound like a company man when I say it, but one way is for the masthead of the site to start mattering again; and for people, when they are judging whether or not they believe a story and whether or not they trust it, to partially base that on whether or not they trust whoever is reporting it. I like to think that the *Guardian* readers, by and large, trust the *Guardian* stories, in part because they are from the *Guardian*, because we have a several-hundred-year reputation for doing that and for providing trustworthy content.

What seems to be lacking is the opposite side of that, the moment of, "Hold on. I have never heard of whoever is reporting this before. Should that be a red mark? Should I hold my fire before repeating this to friends and family?" That may be a cultural thing that will pass. We are still quite early in this. We are very early in the majority of the British polity gaining a substantial proportion of their news from the internet and, beyond that, from social media. It may be that people will just learn and change their patterns. That is a very hopeful, optimistic view of things, but I would almost rather sit on the side of optimism than on the side of a lot of potential interventions like state bodies or the large platforms having to verify whether things are true or false or algorithms and machine learning systems trying to learn automatically to verify whether or not a thing is true or false.

If I, as a journalist, go out and interview someone and they say something new to me and I publish it, broadly there is no automatic way of verifying that. It is the nature of reporting that, to a certain extent, you are taking it on trust from me that I am accurately reporting what I was told. You cannot send an algorithm off to see if that has been reported anywhere else, because I was the first person. You cannot read those comments and then compare whether or not what the person was saying stacks up next to a Wikipedia article that was on the same topic, because the person said it and that is the news story. Reporting has come down to trust for a long time. Sites, companies, journalists and individuals who lie tend to get caught out and that has a damaging effect on their trust going forward. I hope that that will continue to be the case in the online world.

Viscount Colville of Culross: I do admire your optimism very much indeed. It does not seem to be going that way. It seems that there is more and more fake news taking place. I have been a reporter, and when you interview someone you do make sure that what they say has some fact and some truth to it. That is the point of the media: you mediate it and decide whether or not there is some basis.

Alex Hern: On that point, if I may clarify my remarks, I mean that the very fact that person said something has no external source of fact-checking. If someone accuses me of making up a quote from you because they cannot find that quote anywhere else, that is not mechanically checkable.

Viscount Colville of Culross: In a world in which we are seeing fake news that seems to be growing exponentially, contrary to your optimistic view, is it not about time that we had some sort of intervention and some sort of determination that there should be some fact-checking that, "Yes, this should be allowed to go viral"?

Alex Hern: That would be hard. That is effectively the issue here. We say "go viral"; we are talking about social media mechanics. Fake news can come from any individual user on any one of a dozen or so social networks. It is not clear to me what checking there would be if we are to continue to have social networks.

Matt Reynolds: My fear is that a lot of the popularity of things that do go viral or the people who say these things is precisely because they are not part of those organisations and they are outside of that bubble and that type of thing. Although I completely agree with Alex that the idea of authority in a masthead is something I believe in and I would hope, broadly, people come around to again, I think that a lot of what we are seeing is a very direct reaction to that. Trying to put another authoritative wraparound on that would not necessarily solve the problem because I do not always think that people are critiquing it in the same way. I do not always think it is a lack of information. This is a problem with the wider public debate: that it is about being acerbic, it is about being contrary and it is about being different, and actually contextualising it with facts might just not help. It might just seem like another authority that you can ignore. Sorry, I realise that is not a solution. That is the pessimistic side, I guess.

Q158 **Baroness Kidron:** I really wanted to ask you to think about it in a slightly different way, in terms of whether you have any attitude towards the design of service. For example, a YouTube insider recently said that 70% of YouTube videos are shown on the "recommend" button. That means that YouTube has an immense power in the direction of travel of what people are seeing. We also know that those things get more and more extreme. If you start as a teenage girl on a diet site, you end up on a pro-ana site and everything else. We appear to be discussing it as if there is Person A saying one thing and Person B saying something else that is true and they have an equal chance. I really would love you to all say something about the design of service and what responsibilities lie in there, because that does seem a more fruitful place for regulation.

Alex Hern: To be clear, it is that last aspect—whether or not it is clear for regulation is my problem. There are a lot of things that services can do to help with this. Facebook, for instance, has made strides in this direction but for a long time, and particularly in 2016, at the height of or birth of this fear of fake news and misinformation, Facebook radically deprioritised information about where the news was coming from, about what site the link was going to and emphasised information like which of your friends had shared the story and what they had said about it. That strips all of the anchors of trust that I was talking about earlier: the fact that it comes from a credible news organisation, the fact that the original headline was written by a professional journalist, and instead it replaces those with its own sources of trust: this comes from one of your friends and they, until recently, had the ability to rewrite the headline on the link, which is a terrible idea for a news service.

All of that does not help. Facebook has made strides in this direction. They have improved that but they still prioritise the person who shared it because they are a site that is increasingly about fostering connections between friends and family, rather than connections between the corporate world and individuals.

Baroness Kidron: When they are fostering friends and family in a way that creates ethnic cleansing in Myanmar, is there not a responsibility within the design of service about quality of information, et cetera?

Alex Hern: There is, but if there is a more obvious criticism about Facebook in Myanmar, it is that Facebook does not have any staff in Myanmar. Facebook launched in Myanmar without bringing moderators to Myanmar. That feels like a very obvious first step before we start talking about legislating design of the service.

Mark Bridge: There is a responsibility. This is based on algorithms. All of this comes down to their algorithms, which again are a black box. We do not know how they work. There needs to be more transparency on how they work.

On fake news and misinformation, brands like *Wired*, the *Guardian* and the *Times* do retain a lot of trust. However, if you are a smaller player coming out now, and you are decent and doing the right thing, you are going to suffer because people do not have that confidence in you, because of the fake news. The smaller, less known journalism outlets are the ones that are going to suffer more.

Education is really important in this. We have a programme going into schools showing them how journalism is done, how facts are checked and those kinds of things. Again, you have to prepare people, so there needs to be work in schools to get kids familiar with this stuff.

The Chairman: We need to move on to another equally fascinating subject area, which is market concentration.

Q159 **Lord Gordon of Strathblane:** In a way, for all that one might deplore the way internet companies gobble up potential competitors, it does seem almost inevitable that once you have acquired a 51-49 lead in any segment, it very rapidly becomes 90-10, or almost total dominance. That total dominance sometimes can act in the public interest as well. Can you envisage Google being split? A to L, you use Google; N to Z, you use something else. It is kind of unthinkable, is it not?

Alex Hern: I can easily imagine a Google being split so there is a search engine, an email service and a video hosting site.

Lord Gordon of Strathblane: Take that slowly.

Alex Hern: A search engine, an email provider and a video hosting site. If one were to sit down and decide to split up these companies, first, one would have to be either the American Government or the European Union, because there are very few other people who could enforce such a change; secondly, there are clear lines of cleavages. These are large conglomerates. They are not an individual service. Facebook would split very easily into Facebook, Instagram and WhatsApp. Google would split very easily.

Lord Gordon of Strathblane: If we concentrate on Google just for a moment, might it not then lead to you having to pay for any search? Search itself cannot be monetised. They get their revenue from the Gmail and other things.

Alex Hern: Search itself is actually extraordinarily profitable for Google. In terms of search adverts on some topics, a single click can sell for $70 or $80. A search indicates a desire on the part of the customer to find information about that sort of thing. Most obviously, if you search for something like how to buy a car, you are a very obvious target for advertising about how to buy a car, far more obvious than almost anywhere else in the pre-internet age. Search is extremely monetisable. There are areas of Google that probably are not, and that are cross-subsidised by it. One way of looking at that is that is the benefit of running a monopoly: you have a lot of money to cross-subsidise extension into other areas. I am not wholly convinced that that is, in the long term, good for a competitive marketplace and broader innovation in the technical sector.

Mark Bridge: I agree with that. At the moment, as I think Matt said earlier, I use Facebook and WhatsApp—most of us use Google services and Facebook absolutely all the time. All the harms we have talked about linked to these companies are magnified by this ubiquity. The volumes of data that they can collect through this, and the hold they have on every aspect of our lives, again raises all sorts of concerns.

Matt Reynolds: If you are looking at the situation of Google, where Google has leveraged its position to squeeze out competitors on Google Shopping, it was fined for that; it continued to do it up until now. While I agree that scale in the abstract sense is good for me because I can search, do not pay for it and that type of thing—so I agree it has been useful in the same way as the internet is useful—I do not trust those companies not to leverage their power to squeeze out competition in other areas, which is ultimately to the detriment of the users. Yes, I am pretty cautious on that.

Lord Gordon of Strathblane: Mr Hern, you said that Google could be split up. Do you think there is a moral difference between Google using information on my taste from what I search for on the search engine and them scanning my Gmails to see what I have said I happened to like to friends so that they can advertise to me?

Alex Hern: One could argue that there is in that the search advertising is more based on an express desire to see a certain type of information, which ideally search adverts are then presented against, whereas email scanning to present adverts is much more passive. I should note that Google no longer scans emails to present adverts. It did for a long time. They changed their policy on that, broadly, it appears from the outside, because they were not making that much money and it was very bad in PR terms to mechanistically read people's emails, so they ducked out of that market.

The Chairman: Baroness Chisholm, you might have a partial solution.

Q160 **Baroness Chisholm of Owlpen:** You all have talked about the clustering of power and centralisation. We have heard before in this Committee about the dominant platforms and how they benefit from their extensive data silos. I wanted to ask you whether more data portability could help control the power that dominant platforms exercise over personal data.

Matt Reynolds: I agree that data portability should be a fundamental right and you should have the ability to do that. It would very useful if you could say, "I want to download all my photos", which you can now do under GDPR, or, "I want all the information they have about me". I am not that optimistic that data portability would enable the creation of a new Facebook. If we are looking at the scale that Facebook is—2.2 billion people—why are you on Facebook? You are on Facebook because all your friends are on Facebook. You are not on Facebook because you can take that away. Maybe if I could take all of my friends with me and I know they would get that, perhaps it would be a positive thing. Fundamentally, a lot of these things are useful because of the scale, and they leverage that scale more than they leverage the cumulative data to keep people in. While I agree with it in principle, I do not necessarily feel that confident that it would actually change much.

Alex Hern: It is certainly true that the lack of portability has made it harder to build a competitor. The most famous example of portability helping is that Instagram grew as an adjunct to Twitter. For a lot of Instagram's early days, you would sign up on Instagram, it would scan your Twitter followers and see if there was anyone on Twitter who was also on Instagram and you would follow. That was great for building a social network. I am not convinced that in the internet of 2018 the largest social networks would be easy to compete with if only for data portability.

Instead, we should sit down and say that in the market that Facebook is in, it is quite hard to conceive of a competitor coming at it head on and taking it on. Rather than trying to enable a Facebook competitor to build up and use data portability to create competition, maybe we should instead say, "Fine, Facebook has a natural monopoly; the network effects mean that it is extraordinarily valuable and any competitor would really struggle to deal with it. What does that entail for regulation? How does Facebook being a natural monopoly change the Government's responsibilities, or the responsibilities of Governments in general, in shepherding it and protecting its users?"

Mark Bridge: In principle, it is a good idea. Again, I am not optimistic it will be that helpful. Sir Tim Berners-Lee is creating a new platform at the moment where your data is stored in a kind of pod and then different services and different apps get access to different bits but you control that; you see what data is there in your pod and you let an app have a certain amount of that data. It will be very interesting to see how that works out. If that works, that is fantastic. Again, the big incumbents, Facebook and Google, are so convenient. That is the thing: people will trade a lot for convenience.

Baroness Chisholm of Owlpen: Matt, you talked earlier on about how the big platforms are reaping the benefits of their scale. Do you think that should also bring some form of responsibility? Should they step up to the mark, basically?

Matt Reynolds: Yes, undoubtedly. It has to be that. There should be a very high expectation that once we have decided what they should do, they should be held to it and face the penalties if they do not meet that.

I would add to Alex's point. He talked about natural monopolies and Facebook not having a head-on competitor, which I completely agree with. We should also be thinking about what the next platform is. What about in the home? At the minute, look at the companies that are creating the devices for voice communication in the home: Google, Amazon, Facebook and Apple. The reason is because you can leverage your dominance in one market to then get the second one. Rather than thinking about how you create a competitor to Facebook, perhaps we should also be thinking about how we make sure that the next platform is opened up. Maybe that is not about personal data portability but it is about training data and enabling people to develop these things. At the minute, Google is thinking about protecting search but it has search. It is thinking about what people are going to be doing in 20 years and how it can capture that. We should be thinking about how we keep that field open as well.

Alex Hern: On that note, with hindsight it is very easy to say that the single greatest failure of tech regulation in the past decade was allowing Facebook to acquire Instagram. Instagram was probably the greatest risk to Facebook's monopoly that the internet has seen to date. It was succeeding in precisely the way we have talked about: it was not coming at Facebook head-on. It was slicing off a part of Facebook that people engage with very strongly, which was the photo-sharing part, and creating a social network that could quite healthily run parallel to Facebook. Facebook bought it for $1 billion, and then bought WhatsApp later on for $13 billion, and two potential avenues of quite fierce competition with Facebook were cut off. Hindsight is wonderful.

The Chairman: We need to move on. We always finish with a little bit of Brexit—it is the nature of this place; we have not got away with it. I am going to ask Baroness Quin to read a question to put on the record and then I will ask our witnesses, if they will, to reply in writing to Baroness Quin and the Committee.

Baroness Quin: As the Chairman says, it is impossible to be in the Palace of Westminster for a meeting and not hear the word "Brexit" uttered. What effect do you think the UK leaving the European Union will have on the regulation of the internet? Will the UK lose influence as a result of not having a seat at the table? What do you think the overall consequences of that would be? If there are negative effects, how can they be mitigated in the future?

The Chairman: The clerk will confirm that question to you and, if you would be good enough, we would ask you to just send us your thoughts on that. Your evidence has been very helpful to us. You have answered some questions and raised some other ones, and you have explored some areas that are very interesting and useful to the Committee. When you write to us, if there is anything that you feel that we might have considered or that you would have liked to have elaborated on, your thoughts would be very welcome and will form part of the evidence before the Committee. Mr Bridge, Mr Hern and Mr Reynolds, I thank you very much for giving evidence to the Committee today.

Dr Yohko Hatada – written evidence (IRN0082)

Written evidence submitted by Dr. Yohko Hatada, Founder and Director of EMLS RI (Evolution of Mind, Life and Society Research Institute). www.emlsri.org
Dr. Hatada's core interest is for individuals to realize and maximise their own potential in life through self-understanding, supporting political economical social systems; based on researches in Evolutionary Developmental Neuroscience (Oxford University UK, D.Phil), Cognitive Neuroscience (Columbia University US), Adaptive Multimodal System Neuropsychology-Neuromodelling, Neuro Correlate of Consciousness study (INSERM Fr, UCL UK), Buddhism system (Tibetan Sakya School, Jamyang Lhamo). Dr Hatada is co-author of European Parliament Science Technology Options Assessment report on "a governance framework for algorithmic transparency and accountability", Registered Policy Secretary for MPs in both Houses of Japanese National parliaments and worked at the Japanese Ministry of Economy, Trade and Industry.

Q8. What is the impact of the dominance of a small number of online platforms in certain online markets?

1. Democratic processes are being eroded by the business models and their practices of few international online platforms due to lack of speedy vision-driven regulations.

We must understand the nature of the internet in the current technological revolution in the context of global civilizational evolution.

2. I therefore suggest the necessity of fundamental paradigm shifts on several accounts.

[1]. The internet and online platforms must be recognized and protected as public utility.

[2]. As a, last line of defence, we must build whistleblower systems with total encryption as means for exposing corruption within the organizations, as 4th estate.

[3]. Healthy, neutral and non-interfering social media platforms are needed to provide a democratic feedback loop from citizens with constant active engagement as 5th estate societal power structure.

3. I present two perspectives (1), and describe the nature of current technological revolution with online platforms (2). Finally I discuss and suggest their remedies (3).

1 Current governing situation and recent political nature of incidents in democracy

4. Even though all online platforms have in common that they are (primarily) internet based services, the market segment that online platforms are active in varies significantly. Amazon and Ebay represent retail markets, which are largely covered by the Enterprise and Regulatory Reform Act 2013 and monitored by the competition and Markets Authority (CMA). Google (search) and social media platforms like Facebook, Instagram (owned by Facebook), Twitter, Snapchat etc. more closely resemble media organizations but are so far not significantly regulated by Ofcom.

5. a). Democratic processes of elections and referenda have in recent years been shown to exhibit significant vulnerabilities to interference through manipulation of social media. We are losing our sovereign societal foundation unless this "political erosion" is stopped. Liberal democracy is vital for nurturing diversity and healthy development for all and for our long-term future. The urgency of countering 'election hacking' was recently underlined by the formation of a coalition of former statesmen from Europe, the US and Mexico[817].

6. As revealed by whistle-blowers, investigative journalists and subsequent questions by the Commons DCMS committee inquiry on Fake News, during the Brexit referendum there were campaigns of manipulation[818]. Thanks to the market dominance of Facebook, companies like Cambridge Analytica / AIQ were able to get access to the information they needed for mass psychological profiling by focusing on this single dominant social media platform and exploiting its eagerness to attract App developers as part of a strategy for monetizing user data.

7. b). More aggressive forms of usage of platforms are surveillance projects linked to governing management for cities and nation states. These could help simplify and speed up the mundane processes for citizens, but also pose dangers like seen in Uber's governing management. Uber was actively collecting data of citizens and could feed this into government surveillance at request from governing authorities. China is ahead of this approach and citizens are rated according Chinese government's criteria[819], a style of Orwellian governance. We are sliding towards such authoritarianism following technological capability and capacity rather than what liberal democratic society should be. Uber is a Silicon Valley international project. Uber is not even profitable. Investors' interests are not even looking at profitability, more experimenting on possibility of world governance by private data / platform corporates and to create a precedent of the world management to overwrite national sovereignties.

2 Nature of the problems of online platform

8. We must be aware of extreme power concentration in online platform development.

[1] https://www.bloomberg.com/news/articles/2018-05-11/anti-hacking-election-group-started-by-ex-u-s-european-leaders

[2] https://www.parliament.uk/dcmscom

[3] https://www.independent.co.uk/news/world/asia/china-surveillance-big-data-score-censorship-a7375221.html

The communication and coordination capacity of the internet provides many layers of innate colonializing forces that are being dominated by only a few people. This innate force must be fought to keep and develop liberal democratic system.

9. The currently 'exploding' Internet culture itself has innate colonializing forces embedded within the information flow regulation that is being done through algorithmic systems.

10. Power deployment in human civilization has historical inertia of colonialization. Starting from communal, then expanding with war, competing to dominating more, rather than respecting each as they are. Internet and online platform regulation and governances are no exception, seen and directly affecting online governance itself in neoliberal capitalism beyond state sovereignty (as exemplified by Investor-State Dispute Settlement (ISDS) clauses in trade agreements), interstate meddling, infrastructure wiper to destroy data (NotPetya[820]), etc.

11. The internet ecosystem is dominated by a few online platforms that are used internationally. All of these are from the US, Silicon Valley, with a cultural mindset of tech innovation and profit seeking, we are losing diversity in various values.

12. We must understand the magnitude on significance on future development of our independent mind and life in democratic societies as a sovereign state. We must use the online platform for building humane democratic with/without connections to physical real world functionalities (governance management, smart city, Big Data information interaction analysis flow feeding into small group of platforms) to in the current technological revolution in the context of global civilizational evolution. I therefore suggest the necessity of fundamental paradigm shifts on several accounts.

3 Suggested remedies and concepts.

13. In order to avoid conflicts of interest that can lead to distortion of democratic information provision. It is vital that online platform providers remain neutral and do not interfere with the flow of information and communication on the platforms.

14. This means there needs to be strong regulation regarding personalization algorithms that affect which content users are likely to notice.

15. There also needs to be strict regulation regarding the types of advertising that are allowed, with a ban on 'promoted/paid for' prioritization of political campaign messaging.

16. Regulation of platforms must be done by multi-stakeholder bodies, not by private sectors by themselves since the users and services have huge impacts and define the communication and information as described in the sections 1 and 2.

[4.] https://arstechnica.com/information-technology/2017/06/petya-outbreak-was-a-chaos-sowing-wiper-not-profit-seeking-ransomware/

17. We international citizens must be able to have and hear to voices of individuals, all organizations, institutions and layers in society, inclusively.

18. This can only be done by treating online platforms as public utilities that mandate highest regulation for best practice and stopping corruption from occurring.

19. All of the above are vital for a healthy liberal democratic development with fair and just society.

20. We must stop the privatization of the internet infrastructure ecosystem, its users and its information flow ecosystem, and online platforms. Internet information flow is a vital component of modern life and international society.

21. The internet and online platforms must be recognized and protected as public utility. This means that information flow is for genuine interest/value, not for profitability through not genuine value creation. The internet serves as utility for democratic information flow.

22. Due to the significant potential that the large online platforms have in manipulating information flows that are vital for society, it is necessary to maintain systems to guard against corruption in online platform working environment. As a, last line of defence, must build whistle-blower systems with total encryption as means for exposing corruption within the organizations, as 4th estate. Without checks and safeguards, no organization or institution can be guaranteed to remain uncorrupted. An internal check system is a "necessary" function in any body. This must become a norm.

23. Healthy, neutral and non-interfering social media platforms are needed to provide a democratic feedback loop from citizens with active engagement constantly as 5th estate societal power structure. All citizens of the sovereign state must inclusively be decision makers. Such citizens as a whole system become "conscious sensors" responding for each other. Then each individual of the sovereign state can feel connected to each other and cared from each other. Such a state is less prone to internal conflict and feels stronger integrity among citizens with conscientious awareness.

May 2018

Her Majesty’s Government - written evidence (IRN0109)

1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

The Internet is a powerful force for good. It serves humanity by spreading ideas and enhancing freedom and opportunity across the world. Combined with new technologies, such as artificial intelligence, it is changing society perhaps more than any previous technological revolution – connecting people, making us more productive, and raising living standards. Unfortunately, the internet can also be misused and has enabled, for example, the spread of terrorist material, child sexual abuse and led to an increase in other harms such as online abuse or cyberbullying.

To ensure that the benefits of these changes are maximised and fairly shared, and that risks arising from these changes are appropriately managed, we need a regulatory and governance framework which is fit for the future. Whilst some instances may involve new regulation, in many cases it means instead ensuring that existing regulation is applied effectively to new contexts; that the regulation of other markets, practices or media is kept up to date to reflect the impact of the internet; or that non-regulatory measures are effectively deployed. For example, through the Digital Economy Act 2017, we introduced the requirement for commercial providers of online pornography to have robust age verification controls in place to prevent children and young people under 18 from accessing pornographic material. Two landmark pieces of legislation have come into force in May 2018 to keep up with changes in technology: The Data Protection Act 2018 and the Network and Information Systems Regulations 2018.

Should regulation be warranted, it must be done with care to ensure innovation and growth can thrive, minimise the risk of unintended consequences and support fair and competitive markets. Regulation will be one of many levers to be used alongside others such as voluntary action, empowering users with information, tools and skills, and keeping industry accountable through common standards and codes of practice. The combination of correctly targeted incentives and a regulatory framework will secure the best of new opportunities and help us to address the challenges and risks that come with an open, free and safe internet.

Digital Charter

The Digital Charter is our response to these changes: a rolling programme of work to agree norms and rules for the online world and put them into practice. Our starting point will be that we will have the same rights and expect the same conduct online as we do offline.

The Charter’s core purpose is to make the internet work for everyone – for citizens, businesses and society as a whole. We want to make the UK both the safest place to be online and the best place to start and grow a digital business. It is based on liberal values that cherish freedom, but not the freedom to harm others. These are challenges with which every nation is grappling. The internet is a global network and we will work with other countries that share both our values and our determination to get this right.

We will be guided by these principles:

- the internet should be free, open and accessible
- people should understand the rules that apply to them when they are online
- personal data should be respected and used appropriately
- protections should be in place to help keep people safe online, especially children
- the same rights that people have offline must be protected online
- the social and economic benefits brought by new technologies should be fairly shared

The Charter brings together a broad, ongoing programme, which will evolve as technology changes. Our current priorities include:

- Digital economy – building a thriving ecosystem where technology companies can start and grow.
- Online harms – protecting people from harmful content and behaviour, including building understanding and resilience, and working with industry to encourage the development of technological solutions.
- Liability – looking at the legal liability that online platforms have for the content shared on their sites, including considering how we could get more effective action through better use of the existing legal frameworks and definitions.
- Data and artificial intelligence (AI) ethics and innovation – ensuring data is used in safe and ethical way, and when decisions are made based on data, these are fair and appropriately transparent.
- Digital markets – ensuring digital markets are working well, including through supporting data portability and the better use, control and sharing of data.
- Disinformation – limiting the spread and impact of disinformation intended to mislead for political, personal and/or financial gain.
- Cyber security – supporting businesses and other organisations to take the steps necessary to keep themselves and individuals safe from malicious cyber activity, including by reducing the burden of responsibility on end-users.

The Charter will not be developed by Government alone. We will look to the tech sector, businesses and civil society to own these challenges with us, using our convening power to bring them together with other interested parties to find solutions.

As we work on the Charter, we are committing to:

- make it as easy as possible for citizens and others to give us their views

- harness the ingenuity of the tech sector, looking to them for answers to specific technological challenges, rather than Government dictating precise solutions

- consider the full range of possible solutions, including legal changes where necessary, to establish standards and norms online

- lead by example, including through our procurement policy and the unique data we hold

- build an international coalition of like-minded countries to develop a joint approach

Internet Safety Strategy

The Internet Safety Strategy is a core strand of work under the Digital Charter. We published a Green Paper[821] in October 2017, and the consultation response in May this year. The consultation highlighted three main issues: online behaviours too often fail to meet acceptable standards; users can feel powerless to address these issues; and technology companies can operate without proper oversight, transparency or accountability, and commercial interests mean that they can fail to act in users' best interests.

The consultation response also confirmed that the Government will publish a White Paper as a precursor to bringing forward online safety legislation that will cover the full range of online harms. DCMS and Home Office are jointly working to set out our proposals for future legislation across the range of legal and illegal harms to draw together different aspects of Government work, including: reporting on progress of our review of platform liability for illegal content; responding to the first stage of the Law Commission Review of abusive communications online; and working with the Information Commissioner's Office on the age-appropriate design code which is part of the Data Protection Act 2018. It will also allow us to incorporate new, emerging issues, including disinformation and mass misuse of personal data and work to tackle online harms. The White Paper will be developed with the engagement and policy expertise from across all relevant Government departments, agencies and public bodies, as necessary.

We will be considering new policy areas on safety that have been identified during the consultation process that warrant further work, including: age verification to assist companies to enforce terms and conditions; policies aimed at improving children and young people's mental health, including the impact of screen time; tackling issues related to live-streaming; and, further work to define harmful content.

Through this process, we plan to work closely with industry, academia, civil society, charities and other interested stakeholders ahead of the publication of the White Paper.

[821] The green paper set out the current regulatory framework applicable to online harms - any behaviour or action that is illegal when committed offline is also illegal if committed online. Existing legislation covering online abuse and harassment includes: Protection from Harassment Act 1997, Malicious Communications Act 1988, Computer Misuse Act 1990, Protection from Harassment Act 1997, The Criminal Justice and Public Order Act 1994, Section 15 Sexual Offences Act 2003 (for grooming), Breach of the Peace (common law offence) and Communications Act 2003. Source: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf

Secure by Design

Other work supporting the Charter includes the Secure by Design Review, which focuses on improving the cyber security of consumer Internet of Things (IoT). This supports a National Cyber Security Strategy objective to ensure that businesses and other organisations ensure that cyber security is built into technology, products and services by design. This also includes the need for companies to reduce the burden of responsibility on end-users. Many IoT devices sold to consumers lack basic cyber security provisions. This situation is untenable - people's privacy, security and safety are being undermined and, additionally, the wider economy faces an increasing threat of large scale cyber attacks. The review was supported by an Expert Advisory Group made up of technical experts from academia and industry, which sought to identify joint Government and industry action required to address this issue. We published a report in March 2018, the central proposal of the review is a draft Code of Practice aimed primarily at manufacturers of consumer IoT products and associated services. We are refining this Code and considering how some of the guidelines can be further placed within regulation.

2. What should the legal liability of online platforms be for the content that they host?

Platform liability

Online platforms need to take responsibility for the content they host and to proactively tackle harmful behaviours and content on their platforms. Progress has been made in removing illegal online content, particularly terrorist material and child sexual abuse and exploitation material, but more needs to be done to reduce the amount of damaging content online, both legal and illegal. As the Prime Minister announced in January 2018, we are looking at the legal liability that social media companies have for the content shared on their sites. The current regime governing intermediary liability is harmonised across the EU through the eCommerce Directive (ECD). Since its introduction in 2002, social media platforms have exponentially more users, but also access to new technologies that give them greater control over the content they display and a greater ability to derive commercial advantage. It is clear that many of these platforms are no longer simply passive 'hosts' and the status quo is therefore increasingly unsustainable - but also that simply applying publisher status would not be appropriate either.

We are committed to examining how the existing frameworks and definitions can be made to work better, and what a future liability regime could look like. This issue is very complex, and we are carefully considering the options and consequences of change. Traditional publishers and broadcasters are held to strict standards in taking responsibility for the content they host, including through broadcast regulations and editorial codes. Applying publisher standards of liability to all online platforms could risk real damage to the digital economy, which would be to the detriment of the public who benefit from them and to the UK's status as a desirable destination for technology investment. This could be through restricting access to their platform services, some platforms or services becoming unworkable and ceasing to operate, or by passing on the increased costs to users in the form of either increased advertising or charging for some services. We must ensure that any reforms support a level playing field and do not disadvantage smaller platforms or create new barriers to entry. We must also ensure we do not incentivise the over-removal of content: our liability regime must strike the right balance between the right to protection from illegal content and the right to freedom of expression. We elaborate on this further in question 5.

We will be working closely with the full range of stakeholders who have an interest in this area, including technology companies, civil society and international partners. International cooperation here is of critical importance. When technology platforms work across geographical boundaries, no one country and no one Government alone can deliver on the international standards required for a global digital world. We will set out more detail on our approach in our White Paper.

Legal and illegal content

The Internet Safety Strategy consultation also raised concerns about the border between legal and illegal conduct online. The Green Paper focused on harmful but potentially legal content and conduct, but the initiatives which we are taking forward currently on a voluntary basis, including the code of practice and transparency reports, will also support the work being taken forward to tackle illegal harms. In addition, DCMS and Home Office continue to work closely together to ensure that we are jointly addressing activities which could escalate to become illegal and how this is assessed. A joint approach is particularly important in areas such as online hate crime and hate speech, where the line between what is legal or illegal can be unclear. Home Office and DCMS will jointly work on a White Paper which will set out our proposals for future online safety legislation that will cover the full range of online harms (legal and illegal).

We are concerned that, especially for children and young people, being exposed to harmful (but not illegal) content can have negative impacts on mental health and wellbeing and we are clear that there is more that companies could do. DCMS are working closely with the Department for Health and Social Care on how to minimise any potential harmful effects that social media and the internet may have on children and young people’s mental health through the forthcoming Internet Safety Strategy white paper.

The Government is therefore clear that there needs to be greater focus on preventing such online content from being published in the first place. This requires companies to proactively deny access to those who abuse their services; to develop and apply advances in technology to automate these approaches; and for the larger companies to share these tools and techniques with other companies.

It is important to recognise that the leading social media companies are already taking steps to improve their platforms to protect their users from a number of online harms, including online terrorist and child sexual exploitation content. They have developed important technical tools and successful partnerships with charities to deliver online safety initiatives - with plans to do more in this area. The growth of AI and machine learning means that algorithms are used to remove harmful content more quickly. These measures are having a positive impact. For example, Google highlighted in their consultation response that 98% of the videos they removed for violent extremism were flagged by machine-learning algorithms, and they have begun to use this technology in other areas such as child safety and hate speech. Facebook has reported that in Q1 2018, it found and flagged around 86% of the content it subsequently took action on, before users reported it. An increase from around 72% in Q4 2017 attributed to improvements in detection technology.

There have been successes without regulation. For example, we have seen real value from our partnerships with voluntary sector organisations such as the Internet Watch Foundation, the UK's global leadership in the WeProtect Global Alliance, and our strong cooperation with the tech sector through the industry-led Global Internet Forum to Counter Terrorism.

3. How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

We have already seen the largest social media companies commit to bringing forward transparency reports, which provide a picture of the actions they have taken in the process of content moderation. Google published a transparency report earlier this year which looked at how YouTube deals with content on their platform. The report specifically looked at how much of the content was removed by automated technology in comparison to trusted flaggers, other users or at Government request. Facebook has also recently published its internal enforcement guidelines for its Community Standards and a first Community Standards Enforcement Report to explain the prevalence of harmful categories of content on their platform, their efforts at proactive identification and the amount of such content removed.

The UK also welcomes the work that the European Commission carried out with the major online platforms. This includes a Code of Conduct for Countering Illegal Hate Speech which has been signed by Facebook, YouTube, Twitter, Microsoft and Instagram. The aim of this voluntary code is to make sure that requests to remove content are dealt with speedily, and the companies have committed to reviewing the majority of these requests within 24 hours and removing the content if necessary. A monitoring exercise conducted in December 2017 showed that the largest platforms had removed 70% of the illegal hate speech notified to them, compared to 59% in May 2017 and 28% in December 2016. Furthermore, the European Commission recently published its Recommendation on Measures to Effectively Tackle Illegal Content Online. It sets out operational measures that Communications Service Providers should take to ensure the faster detection and removal of illegal content online and also features specific, prioritised provisions to curb terrorist content online, which demonstrates the urgency given to this area by the European Commission. This work is supported by the EU Internet Forum that is pressing industry to do more to prevent terrorist use of the internet.

However, the Internet Safety Strategy consultation highlighted that users are concerned about reporting of content on social media platforms. Only 41% of respondents to the survey (66 individuals) thought that their reported concerns were taken seriously by social media companies, showing a lack of confidence that platforms are moderating content effectively. In addition, while the majority of major technology platforms already have terms and conditions which set out rules on the types of harmful material and behaviour which are allowed on their platform, our survey found that 60% (296 individuals) had seen inappropriate or harmful content online, of which 67% had witnessed online bullying, 53% racial abuse and 50% online misogyny. These figures imply that these terms and conditions are either not fully enforced by platforms, or are out of line with what the UK public expects on safety provisions.

The White Paper will set out plans for upcoming legislation that will cover a wide range of online harms, including both harmful and illegal content. Potential areas where the Government may legislate include the social media code of practice and transparency reporting. We will explore the full range of options ahead of the White Paper for how this should be delivered.

Transparency reports

Transparency reports outlined in the Internet Safety Strategy will provide data on the amount of harmful content being reported to platforms in the UK and information on how these reports are dealt with, including what mechanisms they have in place to protect users. By asking companies to provide information on the number of items reported on their platforms and the number of reports which led to action being taken, transparency reports will help us understand how effectively companies are tackling breaches in their terms and conditions. The reports will also ask companies for information on their moderation process and their community guidelines. A draft transparency reporting template was published as part of the Internet Safety Strategy Government response[822]. These reports will complement the EU Internet Forum's existing transparency report on online terrorist content, which G7 countries and a number of key companies have already signed up to.

Transparency reports will also help to evaluate whether platforms have robust appeals and complaints processes in place. It is right for users to have adequate options to understand decisions concerning their content removal and account restrictions. The Government expects social media platforms to have clear and safe processes in place both to implement adequate protections and, equally, to uphold users' right to share information freely. The draft code of practice for providers of online social media platforms calls for platforms to maintain processes for dealing with notifications from users, including best practice such as offering an appeals process to users who disagree with the platforms' decisions on content removal, and the ability for non-users to report abusive content/conduct, for example parents and teachers to report on behalf of young people. These reports will complement the EU Internet Forum's existing transparency report on online terrorist content, which G7 countries and a number of key companies have already signed up to.

Code of practice

The draft code of practice sets out the principles that social media providers should adhere to in order to tackle harmful content and conduct online, which can have negative impacts on users' mental health and wellbeing. By establishing common standards, companies will understand how they should promote safety on their platforms, and users will know what to expect when things do go wrong. Given the differences between platforms, we have developed a principles-based code that focuses on preventing harm. The draft code of practice covers the following broad areas:

- Clear and transparent reporting practices;

[822] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf

- Processes for dealing with notifications from users; including the number of employees that review abusive reports who have mental health training;
- Clear and understandable terms and conditions and the expectation that these will be enforced, including the action taken to prevent anonymous abuse;
- Clear explanations to the complainant about the action taken in response to their complaint ('comply or explain');
- Information about how to report potentially illegal content and contact, to the relevant authorities;
- A commitment to signpost users to useful information, including on mental health and wellbeing, when they experience harmful content, as appropriate;
- Use of technology to identify potentially harmful online content and behaviours.

It is Government's firm view that the code of practice and transparency reports are a means to an end, and not an end in themselves. Our policy cannot be considered successful on the basis that a particular number of platforms have signed up to the code of practice. We instead need to focus on how these initiatives and others create a more positive user experience online. The transparency reports are therefore intended to be an evaluation tool, providing data related to the extent of users' awareness and use of reporting tools, and the levels of different types of complaints about behaviours and content online.
In the coming months we intend to work closely with platforms and 'trusted flaggers'[823] to refine the transparency reports, and evaluate the successful uptake of the code and its impact on industry and user behaviours, ahead of the publication of the White Paper. In particular we will consider any additions or changes to the code to ensure it's achieving its aim of raising the bar on safety online.

We will also consult with businesses to ensure that compliance is proportionate and straightforward for smaller platforms and start-ups in particular – in order to ensure that they are able to bring innovation to market while also meeting their responsibilities and ensuring children are appropriately protected.

4. What role should users play in establishing and maintaining online community standards for content and behaviour?

Online communities involve their users in various ways to establish and maintain their standards for what is acceptable content and behaviour. At a minimum, users should have the ability to flag content that violates these standards or appears to be illegal. The social media code of practice will provide guidance to social media companies on appropriate reporting mechanisms and moderation processes to tackle abusive content.

Efforts by platforms to provide information and tools for users to improve safety and privacy can help empower them to make more informed decisions about their online

[823] 'Trusted flaggers' include independent organisations that have a trusted relationship with the platforms that flag content that they believe violates terms and conditions.

interactions. Consistent and transparent enforcement of community standards by platforms will also help reinforce to users that what is not acceptable offline is also not acceptable online.

Supporting children and young people to stay safe online

Parents and carers also play a role in supporting children and young people online. As set out in the green paper, we are committed to equipping parents with the information to help prevent online harms, and will seek to deliver such information through a wide variety of routes: the Department for Education will share messages relating to online safety through parent and community champion outreach programmes; we will continue to promote the materials which are available and commission the remodelled UK Council for Internet Safety (UKCIS) to identify any gaps in resources so that we can address these; and we are also ensuring that technology companies continue to support parents by developing technical solutions to online harms.

The Data Protection Act 2018 recognises that children require additional protections in relation to their online data, and that is why we have introduced a new requirement on the Information Commissioner to produce a statutory age appropriate design code for online services that are likely to be accessed by children. Among other things, this code will help make sure that websites and applications are designed in a way that makes clear what data is being collected on children, how this data is being used, and how both children and parents can stay in control of this data.

Schools also play an important role in supporting children when they have suffered the impacts of online harms from cyberbullying and exposure to terrorist material, to online abuse or to sexting. Additionally, school staff are increasingly expected to handle online problems that have taken place out of school’s hours. The challenges which are experienced by young people online will be addressed in new compulsory subjects in England, Relationships Education and Relationships and Sex Education (RSE). Supporting schools in teaching online safety will be an important step for children and young people to understand what is and isn’t acceptable online.

We are also ensuring that technology companies continue to support parents by developing technical solutions to online harms. In recent months, a number of recognised companies have launched new products for the UK market. For example, Google recently launched their Family Link app. The app allows parents to create and manage Google accounts for children under 13 years old and offers tools and information, including details on which apps their child is using and the ability to approve downloads.

Supporting older people to stay safe online

The Home Office is leading an Action Plan for Older People to strengthen our approach to protecting vulnerable older people from abuse, exploitation and crime. Work to address financial abuse of older people, including online, is primarily being delivered and driven through the Joint Fraud Taskforce, and voluntary participation by the banking sector, working closely with government, Trading Standards and victim support. The ‘Take Five’ communications campaign, led by the Home Office and UK Finance, equips the public to more confidently challenge fraudulent approaches, including via email or online, with a focus on the over 65s.

5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

The guiding principles of the Digital Charter are that:

- the internet should be free, open and accessible
- people should understand the rules that apply to them when they are online
- personal data should be respected and used appropriately
- protections should be in place to help keep people safe online, especially children
- the same rights that people have offline must be protected online, and
- the social and economic benefits brought by new technologies should be fairly shared

These principles are mutually supportive. We can, and must, have a free and open internet while keeping people safe online – and the platforms have a key part to play on both fronts.

The internet allows for an unprecedented level of freedom of expression and of information, and we value the platforms that support this. The UK is a founding member of the Freedom Online Coalition, a group of 30 like-minded countries which works to protect online freedom and highlight attempts to restrict access.

We are firmly committed to the rights to privacy, freedom of expression and the freedom to access information in line with international human rights law – online as well as offline. We have demonstrated this by co-sponsoring the 2012 UN Human Rights Council resolution and subsequent iterations on the promotion, protection and enjoyment of human rights on the internet. These are essential qualities of any functioning democracy and promoting these values is a key UK priority both at home and overseas. Any interference with these rights must be consistent with the principles of legality, necessity and proportionality. The platforms have an important role in protecting and promoting these rights.

Approach

Through the Digital Charter and Internet Safety Strategy work, the UK Government aims to develop a defined set of responsibilities for social media companies that provide clarity on the safety measures we expect within a well-functioning digital economy. We know there are a wide range of countries tackling the same challenges on the same platforms and we will continue to work closely with international partners, including in the OECD, EU and G7, on this important work. By taking a leading role globally, we will encourage others to align with our approach - we will demonstrate the advantages of promoting online safety within a framework that also protects human rights, in particular freedom of expression.

Our Internet Safety Strategy consultation indicated strongly that anonymous abuse is a particular problem online. Companies need to pay particular attention to taking actions against users that hide behind accounts to abuse others. The Government recognises that this must be addressed whilst upholding the rights of freedom of expression and information. In March last year, the UK supported a resolution in the UN Human Rights Council affirming that measures for anonymity online can be important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of expression and to freedom of peaceful assembly and association.

The Law Commission is also undertaking an analysis of the laws around offensive online communications. It will look at how the Malicious Communications Act 1988 deals with offensive online communications, how the Communications Act 2003 deals with online communications, what "grossly offensive" means and whether that poses difficulties in legal certainty, whether the law means you need to prove fault or prove intention to prosecute offensive online communications, the need to update definitions in the law which technology has rendered obsolete or confused, such as the meaning of "sender", and how other parts of the criminal law overlap with online communications laws. The Government Equalities Office is working closely with the Law Commission and DCMS to ensure that this work considers gendered offensive online communications.

To ensure the balance is right between freedom of expression and the integrity of the criminal trial process, last year the Attorney General launched a Call for Evidence on the impact of social media on the administration of justice in criminal trials. The issues raised in the evidence received are currently being considered and a response will be published later this year by the Attorney General.

6. What information should online platforms provide to users about the use of their personal data?

A guiding principle of the Digital Charter is that personal data should be respected and used appropriately. The Data Protection Act 2018 makes our data protection laws fit for the digital age, in which an ever increasing amount of data is being processed. It empowers people to take control of their data and supports UK businesses and organisations through these changes. It strengthens the powers of the Information Commissioner to enforce the new laws; giving her a greater range of powers to investigate offences and increasing the sanctions she can levy on rule-breaking organisations. And it ensures that the UK is prepared for the future after we have left the EU.

The Act sets new standards for protecting general data, in accordance with the General Data Protection Regulation (GDPR), giving people more control over use of their data, and providing them with new rights to move or delete personal data. In addition, it preserves existing tailored exemptions that worked well in the Data Protection Act 1998, carrying them over to the new law to ensure that UK businesses and organisations can continue to support world leading research, financial services, journalism and legal services. It also provides a bespoke framework tailored to the needs of our criminal justice agencies and the intelligence services, to protect the rights of victims, witnesses and suspects while ensuring we can tackle the changing nature of the global threats the UK faces.

The Act sets the age from which parental consent is not needed to process data online at 13, which reflects the Government's view that online platforms present significant opportunities and benefits for children. However, the Act also recognises that children require additional protections in relation to their online data and that is why it introduces a requirement on the Information Commissioner’s office to produce a age appropriate design code for online services that are likely to be accessed by children. This code will help ensure that children in the UK are able to access online services in a way that meets their age and development needs. It will ensure that websites and applications are designed in a way that makes clear what data is being collected on children, how this data is being used, and how both children and parents can stay in control of this data. The code will also include requirements for websites and app makers on privacy for children.

In developing the code, the Information Commissioner will consult with a wide range of stakeholders including children, parents, child advocates, child development experts as well as trade associations. The Commissioner must also take into account the UK’s obligations under the United Nations Conventions on the Rights of the Child and must pay close attention to the fact that children have different needs at different ages. We are in close consultation with the Commissioner, as well as Baroness Kidron who has been instrumental in the code’s development, to ensure that this code is robust, practical and meets the needs of children in relation to the gathering, sharing, storing and commoditising of their data. The Commissioner will be required to finalise the code within 18 months of the Bill coming into force. We understand the Information Commissioner will soon be launching a call for evidence, which she will use to gather evidence and views from a wide range of stakeholders on the contents of the code. We have previously outlined a list of areas for the Commissioner to consider when designing the code. Our understanding is that this list has not changed and will serve as a basis for discussions once the call for evidence has been launched.

There is greater public demand for greater accountability from technology companies about how data is used. The Internet Safety Strategy Green Paper consulted parents on topics surrounding online safety they would like more information on. Of the 222 parents who responded to the Strategy online survey, 72 highlighted that they were keen to receive more information on personal data protection. Doteveryone’s report ‘People, power and technology: the 2018 digital attitudes report’[824] also highlighted concerns that there is an understanding gap around internet technologies, how data is used and how companies make money.

7. In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

There is significant variety in the business models used by online platforms, but there has been a trend towards providing free content and services that are paid for by monetising users’ personal data, including through advertising. Consumers need to understand what they have agreed to when accepting a contract or privacy notice, but there is evidence that many users do not understand how the services they use are paid for, or how their personal data is used to personalise the service and the ads they see[825].

The UK’s new data protection laws will require consumers to ‘opt in’ to clearly presented privacy policies when handing over personal data and makes clearer that organisations which use algorithms and other techniques to process personal data

[824] http://attitudes.doteveryone.org.uk/

[825] E.g. DotEveryone’s Digital Understanding survey http://understanding.doteveryone.org.uk/

should be able to explain how any outputs are reached. The same laws require organisations to notify individuals when they have been the subject of an automated decision (i.e. one made without human agency) and provides them with the opportunity to ask for the decision to be reconsidered or for a new decision to be taken not based solely on automated processing.

Government is also gathering evidence to better understand the impacts of and transparency around personalised pricing. The recent Consumer Green Paper highlighted that varying prices based on consumer characteristics is commonplace in many markets, both offline and online. However, firms online can access and analyse substantially more consumer data, such as search history, thus making it easier to personalise prices and search. This could save consumers time directing them to well-matched products, as well as saving them money if discounts are offered, but it could also make some consumers worse-off.

In order to create a safer digital ecosystem in the future, we need to influence the development of new and emerging platforms. While there are examples of best practice (see the Internet Safety Strategy consultation), it is critical for developers and designers to take a 'think safety first' approach to embed safety considerations into their product development. We believe that companies must take a more proactive approach, pre-empting potential issues on their platform before they occur. The upcoming White Paper will set out in more detail this approach.

Centre for Data Ethics and Innovation

Finally, the Government is also investing £9m in a new Centre for Data Ethics and Innovation. The new Centre will identify the measures that are needed to strengthen and improve the way data and AI is used and regulated. As part of this remit it will agree and articulate best practice, coordinating efforts with industry and other key stakeholders to develop standards, codes of practice and accreditation schemes. It will also identify steps that are needed to ensure that law, regulation and guidance keep pace with developments in data-driven and AI-based technologies.

The Government is currently in the process of setting up the Centre and has recently launched a consultation on its role, objectives and activities. The range of issues which it will consider as part of its initial work programme will be determined following this consultation, but are likely to entail issues relating to a number of high level themes such as targeting, fairness, transparency, liability, data access, intellectual property and ownership.

8. What is the impact of the dominance of a small number of online platforms in certain online markets?

The digital economy is fundamentally changing the way many markets operate. A key priority for the Digital Charter is to ensure digital markets work well for everyone. Effective competition in these markets leads to the greatest benefits for consumers, driving business to innovate and giving consumers better products, cheaper prices and greater choice.

The Competition and Markets Authority (CMA) is the independent body which has been given powers by Parliament to make sure that competition works across the economy.

Our competition tools are designed to be sufficiently flexible to tackle competition issues across the economy.

However, digital services – particularly those that are free-to-use and funded by advertising – pose challenges to our existing competition frameworks. As set out in the *Modernising Consumer Markets* green paper, the Government will review the UK's competition tools in the context of digital markets to make sure the powers are effective in responding to the new digital challenges. This will form part of our overall competition law review, which will be completed by April 2019.

Where markets are dominated by online platforms and shaped by the network effects that their services create, there is concern regarding the facility of the existing competition regime in tackling resultant market concentration. The review will consider whether the current competition regime is sufficiently equipped to respond to the rapid changes taking place to business models in the digital economy. It is also seeking evidence on how it should address platforms, agglomeration, algorithms and the consolidation of competitors.

Access to data is a key factor in supporting innovative new technologies and facilitating easier consumer decision-making, which in turn are important tools in making online markets more competitive. The right to data portability, introduced in the Data Protection Act 2018, gives individuals the right to request access to and move certain types of personal data between organisations.

To take full advantage of this new right and make data portability a reality for consumers in in a wider range of markets, we have commissioned research to understand how greater portability could make a real difference to competition, and to engage with business to understand what actions are needed to deliver these benefits.

The government has also launched a review into how best to ensure data portability is implemented in a way which supports consumers to access better deals in regulated markets, building on the approach pioneered by Open Banking. The review will seek to identify those regulated markets where data portability can have the biggest impact and how regulators can be empowered to introduce transformative changes for the benefit of consumers.

9. What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

The Internet is a borderless, global communications medium. The UK already takes a leading role internationally, working with like-minded democratic governments to address a range of issues raised by the internet. This includes being at the centre of emerging global discussions on the economic and ethical issues raised by the use of data and artificial intelligence. As the UK leaves the EU, international collaboration will be more important than ever; we will continue to look for partnerships and opportunities for co-operation, bilaterally and multi-laterally through organisations such as the OECD, G7, and G20, as well as continuing to work closely alongside the EU.

The UK will not be part of the digital single market after we leave the EU. As the Prime Minister has said, we are aiming for the broadest and deepest possible partnership, cooperating more fully than any free trade agreement anywhere in the world.
It is pragmatic common sense that we should work together with the EU to deliver the

best possible outcome for both sides in support of the digital economy and online safety. We will look closely at the regulatory environment for digital as part of the negotiations and carefully consider how the future relationship between the UK and the EU can benefit us all. As detailed in the response to question 2, we are committed to working with our partners around the world, including the EU, to understand how we can make sure online platforms have the right level of responsibility for any illegal content they host. This is a complex and challenging issue, and we will be carefully considering the options and consequences of change. There's always mutual advantage in cooperating on digital issues across Europe and that will continue after we leave the EU. Current examples include:

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR) and elsewhere, we continue to engage the EU whilst we remain a member. We are playing an active role in shaping the EU Commission's current work on 'Tackling Illegal Content Online - towards an enhanced responsibility of online platforms'. We are also actively engaging bilaterally and multilaterally with like-minded countries and in various forums as how we can better tackle illegal content together.

The UK remains actively engaged in negotiations to the Copyright Directive where the Council recently agreed its position on the draft text on 25th May 2018, ahead of further political negotiation at Trialogue. The draft directive contains a number of provisions aimed at adapting EU copyright rules for the digital environment, and harmonising practises across member states in order to increase legal certainty in the Digital Single Market. The Directive will enter into force during the implementation period, in which case it will be implemented in UK law. Our future 'alignment' with the Directive will depend on the terms of our future relationship with the European Union.

Net Neutrality is the principle that Internet service providers should enable access to all content and applications regardless of the source, and without favouring or blocking particular products or websites. The EU's Open Internet Access Regulation harmonises legal net neutrality standards across the EU. In addition, it stipulates that each member State must appoint a national regulator to safeguard these standards. The UK national regulator is Ofcom, and the Government strongly supports Net Neutrality. We are clear that users of internet services should be able to access the services they wish to, without unnecessary blocking or slowing down by providers. We have no plans to change the UK's policy on net neutrality.

As requested by the Lords Communications Select Committee to Government officials during private oral evidence on 5 June 2018, below are some of the Government departments and agencies who may be involved in the publication of the Internet Safety Strategy White Paper. In addition, we will work with the Devolved Administrations where appropriate.

Attorney General's Office

Cabinet Office

Department for Business, Energy and Industrial Strategy

Department for Digital, Culture, Media and Sport

Department for Education

Department for Exiting the European Union

Department for International Trade

Department of Health and Social Care

Foreign and Commonwealth Office

HM Treasury

Home Office

Ministry of Housing, Communities and Local Government

Ministry of Justice

Northern Ireland Office

Crown Prosecution Service

Government Equalities Office

Information Commissioner's Office

The Electoral Commission

National Crime Agency

Ofcom

Security Service

Gambling Commission

Government Communications Headquarters

National Counter Terrorism Security Office

Office of the Children's Commissioner

June 2018

Her Majesty's Government – oral evidence (QQ 183-196)

Monday 12 November 2018

Watch the meeting

Members present: Lord Gilbert of Panteg (The Chairman); Baroness Benjamin; Baroness Bonham-Carter of Yarnbury; Baroness Chisholm of Owlpen; The Lord Bishop of Chelmsford; Lord Goodlad; Lord Gordon of Strathblane; Baroness Kidron; Baroness McIntosh of Hudnall.

Evidence Session No. 21 Heard in Public Questions 183 - 196

Examination of witness

Margot James MP, Minister for Digital and the Creative Industries, Department for Digital, Culture, Media and Sport.

Q183 **The Chairman:** I welcome everybody to this session of the House of Lords Communications Committee. Our inquiry is into regulation of the internet. It is wide-ranging and we will probably report in the new year. I am delighted that our witness today is Margot James, the Minister for Digital and the Creative Industries. We have a wide set of questions for you, Minister. Thank you very much for coming to see us today. As usual, the session will be broadcast online and a transcript will be taken.

Minister, perhaps you could introduce your brief to the Committee and tell us about the digital charter and the internet safety strategy; in particular, whether you think that the various regulators have the resources that are required for them to fulfil their brief. Then we will open it up to some wider questions from members of the Committee.

Margot James MP: Thank you very much, Lord Gilbert, and thank you all for this very important inquiry that you are undertaking. That is quite a broad question to start with. I will be as concise as I can be in my response. As you mentioned, my brief covers digital and the creative industries. That includes technology, telecoms and the vast majority of what would be called creative industries. One of my top three priorities, in a very wide brief, is securing an online environment that is more respectful of users and protective of their rights and security. That is definitely one of my top three priorities.

You asked about the digital charter, which came into being last year. That sets out at quite a high level the principles we want to see embody the internet for our citizens: that it should be free, open and accessible; that people should understand the rules that are applied to them when they are online; that people's data should be respected and used appropriately—obviously that has had a big airing as a topic for debate in its own right this year; that there should be protections in place to help keep citizens, particularly children, secure online; and, most importantly, that the same rights that people have offline must be protected online and that the social and economic benefits brought by new technologies should be fairly shared. We are committed to those principles. The charter is not just established and set in stone. It is there to evolve as the technology evolves, and guides a lot of what we are doing.

You also asked about the internet safety strategy, which falls out of the digital charter, essentially. The sequence of events on this has been that my department consulted through the publication of an internet safety Green Paper last autumn. The Government responded to that consultation and published their response in May this year. At that time we announced that we would be working on a White Paper on tackling and addressing online harms, for publication this winter, and that we fully expected that to be followed by legislation as soon as the parliamentary timetable permitted.

Q184 **The Chairman:** We have heard from witnesses about the role of various regulators in the field. There is a variety of regulators with a range of responsibilities. A number of our witnesses have strongly argued that we need either an overseeing regulator or, at the very least, a body that scans the horizon and that understands new developments in the area of the digital economy, new issues as they arise and new remedies. What thought has your department given to our current regulatory structure and the extent to which it needs to be changed or improved as we proceed?

Margot James MP: We are giving a great deal of thought to that very subject at the moment as we work on our White Paper. A number of regulatory bodies have an online footprint in their day-to-day work: Ofcom, the Advertising Standards Authority, and the Information Commissioner, of course.

There are various regulators that apply their work online, but it is not necessarily either their sole remit or the main purpose of their activity. In the way the regulatory landscape has evolved, in line with the point made in the digital charter—that the same rights that people enjoy offline should be protected online—there has to date been a reliance on existing regulators to apply their work online. However, because the online environment presents several unique challenges, it is felt that there is too much of a gap in the regulatory armamentarium which is allowing swathes of online activity to proceed with very light-touch regulation and, in some instances, no regulation at all.

The Chairman: I mentioned the resources available to the regulators. Do you think the regulators are sufficiently resourced to hire the staff they need in competition with the internet giants?

Margot James MP: The ICO is probably the best live example. We have recently increased significantly the money, human resources and expertise available to the ICO in anticipation of the greater volume of work that is likely to flow from the new data protection legislation.

In that case, I can answer your question with a degree of confidence, but there are other areas where the online world has presented new and far greater challenges than many existing regulators are resourced to cope with and where the answer at the moment is that we probably see a gap in the resourcing. But it is too soon to give you a more detailed and accurate response, simply because, as we are currently working on the White Paper, we have to come to a conclusion concerning what we want to regulate, or what we feel needs to be regulated, before we can decide how best to regulate and therefore what resources such a regulator will require. There are certain questions that cannot be answered just yet, but I reassure the Committee that we are working very hard on all those aspects.

The Chairman: One final question from me. As you contemplate further regulation in the swathes of unregulated areas that you have described—indeed, that implies that you are considering further regulation—how do you balance that further regulation with innovation and issues arising from that set of public policy balances?

Margot James MP: That is a very important question, and we are extremely keen to get that line right. We want to improve people's safety and security online, apropos the principle that what is illegal offline should be illegal online and treated similarly, and so forth. Any measures that we introduce to make citizens more secure online will set clear online-safety expectations to protect users from harmful behaviour and criminality without deterring innovation and growth within the tech sector.

These are both crucial requirements, and we see no reason why they cannot go hand in hand. Our aspiration is to arrive at a point where the online world is similar to the offline world in what citizens can expect and how they can expect to be treated, and where we have a flourishing technology sector, which I am hopeful will be all the more positive an environment commercially while the online world is a more secure place for our citizens. I do not see a contradiction between the two.

Q185 **Lord Gordon of Strathblane:** Minister, it occurs to me that, as you have described, the internet touches every aspect of life nowadays. It is very important to realise that the digital charter is not a one-off White Paper; it is a rolling programme. In many ways, however, the expectation is growing. So many problems have been parked, awaiting the digital charter, that the more you include in it the more people will conscious of what you have not addressed. Undoubtedly, new problems will arise before the ink is dry.

Margot James MP: You put the point very well indeed, which is why anything that we introduce under the auspices of the digital charter, particularly things that we introduce into law ultimately, need to be mindful of the fact that, if we regulate, we are proposing essentially to regulate a moving target. Things evolve very rapidly with new technology; there is no doubt about that. So we need a flexible approach.

There is another point, which is that the evolution of technology will in part provide the solutions that we are looking for. Technology itself will play a huge part in the improvement of the online environment.

Lord Gordon of Strathblane: On the question of potential legislation, while accepting that it is not a given that there will be any, it is probably likely that at some point in the future there will be a necessity to legislate. You have already alluded to the fact that it is a moving target.

Frankly, Parliament is not best equipped to deal with something like the internet. We face the choice of giving Ministers Henry VIII powers, which MPs are not terribly keen on, or having them legislate ponderously, probably over a year, through both Houses, at which point the target has moved on. How do we cope with that?

Margot James MP: Certain things move on. Technology itself enables more rapid communication, and sometimes more anonymous communication. There are all sorts of things that technology enables and that will continue to evolve, but that does not necessarily mean that we should or need to sit back and be content with the current regulatory environment. Simply because a sector of society moves at pace does not mean to say that it should not move at pace within the law and within an acceptable regulatory environment.

Lord Gordon of Strathblane: Witnesses at various sessions have thought that it might be helpful for the department to have a horizon-scanning body, a sort of forum that perhaps elects its own chairman and advises the Government of X, Y or Z problem that is on the horizon so that we can take pre-emptive action and prevent the problem arising in the first place, rather than take remedial action later. Do you see that as a potential advantage?

Margot James MP: A sort of technology observatory sounds like a very good idea. We have officials in my department who are tasked with assessing and staying across emerging technologies. The team is highly qualified, which enables us to get the best-quality advice. Of course, we have a fantastic university sector in this country—four of our top 10 universities are in the global top 10—and there is a huge amount of research. So I think we have the benefit of horizon scanning, but there is no reason why it should not be more formalised in the manner that you suggest.

Q186 **Baroness McIntosh of Hudnall:** Minister, I want to take you back to a point of detail in your first answer on the internet safety strategy. You talked about the consultation—and, by the way, this has nothing to do with the question that has just been asked.

I was a bit puzzled when I read the evidence from your department about the size of the sample from which you were drawing your conclusions about the numbers of people who were concerned about this or that element of safety. Can you tell us the scale of response to your consultation, both the numbers and your expectations?

Margot James MP: I will have to write to the Committee with the precise numbers which the consultation produced. I have tried to interrogate this base of respondents myself. I will redouble the set of inquiries that I left with officials a little while ago and write to the Committee.

I noticed that Ofcom has also done some research—in the last couple of months, in fact. It published it, I believe, in September. From memory, 55% of respondents to the Ofcom consultation revealed that they had observed or been the victim of an unpleasant or illegal action online and thought that there should be better regulation of online platforms.

Baroness McIntosh of Hudnall: My point is that percentages can be misleading—

Margot James MP: Indeed.

Baroness McIntosh of Hudnall: —because if the sample was small, the numbers will not be particularly telling. It would be helpful for us to know, because in necessarily persuading for example the tech companies that there is a serious public concern about this, a small sample might not help.

Margot James MP: I will definitely write to the Committee with the numbers. I do not know whether I am reassuring you, but I looked at that research and thought, "Fifty-five per cent think that social media platforms should be better regulated. That's very interesting", because I thought it would be more like 80% of the people I speak to, and more. Hardly anyone I speak to does not think that social media platforms would not benefit from better regulation.

The Chairman: Thank you for offering to send us that information.

Q187 **Baroness Chisholm of Owlpen:** Leading on from that, I have two questions. One is about the Government's proposal for annual transparency reports on social media platforms. Another is whether the Government's proposed social media code of practice in the internet safety strategy will look at the important area of platform takedown and the appeal and complaints procedure.

Margot James MP: Yes. I should preface my answers with the point that we are working on these approaches and they are evolving. We published a draft version of the statutory code of practice in May this year. Since then we have been consulting a wide range of stakeholders on the code of practice and we are currently developing a revised version of the code. We anticipate that it will set a clear and common approach to online security, that it will help companies to understand how they should promote safety and security on their platforms, and that it will make it clear to users what they can expect when things go wrong and when they report problems they have experienced to the relevant platform.

Social media transparency reporting is an expectation that we will set social media platforms and other relevant internet companies with regard to their publication of the number of complaints they have received, the nature of those complaints and their response to them. We see the transparency agenda as very important, and it is what we anticipate coming out of this.

Baroness Chisholm of Owlpen: Surely one of the most important things must be that the appeals process is easy for a person to be able to go through, that they can feel they will get some answers and that the large platforms cannot hide behind it.

Margot James MP: Exactly. That is completely the purpose. At the moment, many systems for reporting are far too opaque and the response mechanisms are far too haphazard. During some of the consultations that I have led myself, I have seen a tendency for users not to bother to report problems because they anticipate that nothing will be done. We have to achieve a cultural change through this new approach when it comes into being.

Q188 **Baroness Kidron:** Perhaps I might say at the outset how delighted I was to hear you say in your opening remarks that you want an online environment that is "respectful of users" and delivers on their rights and security. That is so refreshing, because we hear so much about safety, and actually this aspiration for a beneficial technology is very welcome.

My questions are about algorithms and the approach to regulating them, perhaps to get a little more understanding about what is under the bonnet. So my first question is about the approach. My second is: what is your feeling about the use of things such as impact assessments and universal standards—things that are widely used in other technological situations?

Margot James MP: Algorithms are becoming much more the topic of discussion in relation to the hidden biases and directions they are setting, which are not necessarily transparent to the end users. We feel that there should be greater accountability for and transparency in how these algorithms are developed, established and set, so that people have a better idea of how they and their data might be affected by them. This is an area we are looking at in our development of the White Paper.

In addition, we are establishing—this month, actually—the Centre for Data Ethics and Innovation, and we will ask it to assess the impact of algorithms in certain areas to make sure that the public are better informed about them.

There is not just the new centre. The Competition and Markets Authority has been asked by the business department to look into the effect of algorithms in certain sectors of the economy, under the auspices of the consumer rights Green Paper published by that department in April. I will give the Committee one example of what I believe the CMA is looking at in the aviation sector, where algorithms are deployed to allocate seats on aircraft.

Some airlines have set an algorithm to identify passengers of the same surname travelling together and have had the temerity to split those passengers up around the plane, and then when the family ask to travel together they are charged more. That is an example of a very cynical, exploitative means of deploying algorithms to hoodwink the general public, which these various bodies, such as the CMA and the new Centre for Data Ethics and Innovation, are going to get on top of, I trust.

Baroness Kidron: Can you see a direction of travel in which, rather than finding cynical or bad practice and then punishing it, we actually set—in advance, pre-emptively—certain levels of behaviour that are expected and will be regulated in that sense?

Margot James MP: The answer is yes, and I very much agree with what is behind your question. It is not enough for us to criticise bad performance, although it is very important that we root it out, hold companies to account and expect better of them. As you suggest, it is very important to the realisation of all the benefits of technological change, which are so manifest, that these benefits can flourish and that citizens can take advantage of them with confidence. That is the happy state which we aspire to.

Baroness Kidron: I would like to ask one very specific thing. I know you have spoken publicly on this yourself. Tristan Harris of the Center for Humane Technology speaks a great deal about the attention economy and the interruption of free will by algorithmic methods trying to get our attention, hold our attention and reward us for our attention in what might be considered bad-calorie ways. Is this in scope as an issue, as a harm? Is deliberately creating compulsion a harm?

Margot James MP: I think it should be in scope, and I will endeavour to make it so in my work towards the White Paper. You touch on something that is really at the nub of so many of our problems with social media platforms: the fact that the algorithms are exactly as you have described. For instance, if you key in "weight loss" on YouTube—or another platform; I do not want to single one out—you get bombarded with great volumes of the same material. Of course, if someone is vulnerable and has any mental health or addiction problems, or anything like that, that can make the situation very much worse. There are a legion of different examples that we could deploy on the same theme, which is that these algorithms need far greater transparency and companies need to be held more to account for their deployment.

Baroness Kidron: And perhaps a bit of oversight on the recommends.

Margot James MP: Yes, exactly. I have huge respect for the Center for Humane Technology. I think it is doing fantastic work. I hope to be meeting it next spring when I visit America. It is definitely on my list of organisations I want to see.

Baroness Kidron: Excellent. Thank you.

The Chairman: Can I return to your example of the airline seating scam to pull two things out of this?

Margot James MP: Yes.

Q189 **The Chairman:** When we go about trying to deal with that issue by regulation in one form or another, will we try to regulate the behaviour of the airline in conducting this scam in the first place or will we try to address it through regulating algorithms? It seems to me that actually that may not be an algorithm and that it could easily be done without an algorithm. The definition will have changed.

If we approach it by trying to address algorithms, we may well find that the airlines are still carrying out the same behaviour but using a different methodology. Are we looking at a whole range of newly emerging behaviours that we are going to try to regulate, or will we try to tackle it through regulating the technology?

Margot James MP: That is a really good question, which focuses the mind. You are right that technology enables greater opaqueness, but it is not necessarily always responsible for the motivation of the company to try to cheat its customers, which in essence is what such an airline is doing.

We need to dig back to setting greater standards of corporate responsibility so that companies are not manipulating and hoodwinking customers and feeling that that is an okay version of customer service, which it is not. It is not the technology's fault; it is the poor standards of corporate governance in whatever organisations are culpable in that area.

This strays into areas of corporate governance and consumer protection, which are the preserve of the business department. Having been a Minister in that department, I am quite aware of what it is trying to do and I applaud it for that, but just regulating the technology will not get to the root of the problem.

The Chairman: I come back to this, because it has emerged from this inquiry that there are two aspects of regulation that we are looking at: regulation of the digital economy and regulation in the digital era. It is an example of where regulation is not keeping up with the way the world is changing in the digital era. It is not itself a digital issue. Bad behaviour has greater consequences because of the pace and capacity, but it is not itself a technical issue.

Margot James MP: No. I agree with where you are coming from on this. Your question should inform the development of our White Paper and our thinking about regulation. I have already said that if we do regulate, we intend to do so very sensitively, with an eye to encouraging innovation as well as to making the online environment a more secure place for citizens.

But I take your point that a lot of what we are trying to improve is stuff that might have been easier to detect in the offline world than in the digital world. Because of that, the consumer needs to be empowered but also needs protection, because it is easier in the online world to act without people realising what your agenda is.

Q190 **Lord Goodlad:** Minister, my question is about the safe harbour provisions in the e-commerce directive. Do you think that after Brexit this country ought to repeal the safe harbour provisions of the e-commerce directive?

Margot James MP: I am not quite sure I follow your connection with the safe harbour provisions, which, as far as I understand it, apply to an arrangement that the European Union has with the United States on data protection. Of course I am familiar with the e-commerce directive, which mimics to a certain extent the provisions in the United States by enabling online platforms to operate without liability for the content on their platforms. Is that the gist of what you would like me to address?

Lord Goodlad: Very much so.

Margot James MP: Okay, thank you. The answer is that we are not seeking a hasty retreat from the e-commerce directive. I should preface everything I say by saying that, as with everything else, what we do post Brexit is all a matter for the negotiations and the deal.

What I can say is that more can be done within and under the e-commerce directive. The e-commerce directive permits companies to be liable for hosted illegal content once the company is aware that that content is on its platform. Then, if it does not remove that content expeditiously it is within the preserve of member states to have legislation to fine such a company.

Indeed, Germany brought this into law at the beginning of this year. The German Government passed a law that makes platforms liable for any illegal content found on their sites and they are subject to substantial fines if they have not taken the content down within 24 hours. There is an interesting aspect here, which I think is important. The company's liability takes effect only once it becomes aware that the content is on its platform. That enables the company to have a fairly reactive policy in place, and to outsource the policing and detection of all this illegal content to the third sector, to Governments or to the police. Actually, some respondents to our consultation have told us that that is a derogation of duty and ask: why should the public purse pick up the bill for that sort of investigation?

Baroness Kidron: You have answered half of my question. "Once it becomes aware" is the problem, is it not? We have found, particularly in relation to children, that these companies are expecting pre-schoolers to police the internet, as it were. That is unacceptable. I do not mean to put you on the spot, but there is the idea of a duty of care, which we will discuss in the House later this evening. Do you think that a duty of care would match the liability question? If we introduce duty of care, do companies then have a duty of care irrespective of the liability question of the e-commerce directive?

I suppose the other thing is that, if they insist that it is only illegal content that they are responsible for, does that push Governments into creating more illegality instead of having a better cultural and—to quote you back at yourself—"respectful" environment?

Margot James MP: We are certainly looking at duty of care as one potential solution we develop the White Paper, for some of the reasons you have just set out. I do not want us to get ahead of ourselves here, but I suspect that ultimately it will not be a one-size-fits-all solution. There will be various ways of approaching the challenge of getting a more respectful online environment and protecting people's rights.

You make the point about the distinction between content that is illegal and content that is harmful but not necessarily illegal. There is a grey area between the two, of course, as there is offline. For those reasons, I doubt that one solution in the law will be adequate. We will probably look at a panoply of measures that will ultimately improve the online environment for everybody.

The Lord Bishop of Chelmsford: I resisted coming in earlier on the content moderation issue, but I will just try this one out. When a cinema chain is showing a film, it does not wait for somebody to complain that the content was completely inappropriate; it has filters and processes that are governed and regulated, so it decides what is shown and then gives helpful and widely understood recommendations about who the film might be suitable for.

Could not the clever algorithms that muddle the seats on the plane and then charge us to sit next to our loved ones—that might be a mixed blessing, but anyway—

Margot James MP: You might be happier with the original seat.

The Lord Bishop of Chelmsford: It depends how long the flight is, but that is another matter. Could not those clever algorithms do a similar job before the content goes up?

Margot James MP: You raise a very good point. One of the consultation round tables that I will host later this year involves more technology experts so that we can get an idea of what is possible.

I should have mentioned earlier—you may already know—that we are working on the White Paper jointly with the Home Office, which has had quite considerable success in removing huge amounts of terrorist content. At first it was expected that terrorist content would be taken down within one or two hours of it going up, but now it is expected more and more that the algorithms and other technological solutions will identify material as it uploads and immediately take it down. That is an excellent example of where voluntary working with the internet companies has produced results, and we want to see more of those approaches in other areas of illegality and harm.

On your cinema analogy, it occurred to me while you were speaking that, although you would not expect the cinema to show stuff and then warn people—I think that was your analogy—neither would you expect the cinema chain to be judge and jury over what it should flag up. That is something else that we want to tackle in our White Paper. In fact, a number of companies are keen for the boundaries to be set. Some companies do not see it as their role to decide what content crosses the line and what does not, and it is unusual that they have been permitted to get to this point.

Q191 **The Lord Bishop of Chelmsford:** It is also the case, as I am sure you are aware, that some of the big players—I will come to this in my set question in a moment—now concede that it is not enough to say simply, "I'm a platform upon which others stand". We have gone beyond that now, so it is timely to be thinking about these things.

I am sorry. That is a comment, which you may wish to comment on, but I will move on to market concentration of the few very big players. What are the benefits and risks to consumers of the concentration of the digital market in the hands of a very few, very large tech companies?

Margot James MP: There have been some developments. The competition law review was announced in the consumer Green Paper, which I mentioned earlier, which was published in April. That review, which will report next spring, will look at whether our powers are adequate in the face of large concentrations of technologies in a few companies, which is what I think is behind your question.

I await that report with interest. It is being driven more by the business department and the Treasury, but obviously my department is keeping a close eye on it. There are moves in the United States to look at this, because a lot of the companies we are talking about are US-domiciled organisations.

I do not have a lot to add at this stage.

The Lord Bishop of Chelmsford: Just to press you a little on this, our competition law deals on the whole with things of economic interest, whereas one of the big anxieties that we as a world have about a few large companies dominating the market is the harm it will do. We have received some evidence on this. Jamie Bartlett at Demos talked about the harm it will do to democracy rather than to consumer welfare, and Lorna Woods, of the excellent University of Essex, told the Committee that competition law does not really account for non-economic interest.

How do we tackle things that cannot be measured economically but where all the anxiety lies?

Margot James MP: Going back to the economic thing for a minute, I mentioned the panel reporting in February next year. My department is directly involved with the business department and is working jointly with it on the digital competition expert panel.

Democracy could, as you say, be affected by the concentration of so much market power in so few organisations. There are various ways in which we are trying to address the potential impact on democracy of some of the consequences of unpoliced activity online, which is a huge subject in its own right. The Information Commissioner reported only last week on the use of data analytics in political campaigning. She said, "The invisible use" and processing "of personal data to target political messages to individuals must be transparent and lawful". She found in her report that at the moment it was not. She found a disturbing disregard for voters' personal privacy, that companies had been wholly negligent and that there had been illegal activity on the part of organisations campaigning in British elections and referendums.

There is great concern, and the Electoral Commission, the ICO and the Cabinet Office are all working in this area to strengthen our defences against the manipulation of people's data in the pursuit of electoral gain.

Lord Gordon of Strathblane: I have a follow-up question. Some of the offline activity involving the media is subjected to a public interest test. Is there not a case for looking at a public interest test in relation to some of the internet mergers that go on?

Margot James MP: The public interest tests apply to critical national infrastructure in the case of companies being acquired by companies overseas. Critical national infrastructure is grounds for a large merger or acquisition being referred to the Secretary of State for Business, so there is some protection there.

In the environment that we are looking at, there may be a bit of a crossover into the duty of care mentioned by Baroness Kidron. It sounds to me as though there might be potential for looking at both these areas within our deliberations.

Q192 **Baroness Kidron:** I want to go back to the question of economic value and data. One of the big moves in America, particularly among the people whom you may go and see in the spring, is in recognising that data itself has a value. When the Committee was doing its inquiry into advertising, we really got behind the idea that if only we publicly attached a notion of value to data, first, it would be harder for it to be so rapaciously taken away from us because it might have some value and, secondly, the existing levers, such as the Competition and Markets Authority, would suddenly say, "Hang on, how is this value being distributed, and should we take a look at that?"

Perhaps it is worth saying that if one wants to see the extraordinary financial value in data, one can look at the companies that have no revenue but a lot of data and see what their capital value is. I am sorry for making such a complicated comment, but has this come up in your thinking more broadly? I am aware that it is the breaking wave in America as an idea.

Margot James MP: Definitely. It is certainly top of mind at the moment.

Going back to the Lord Bishop of Chelmsford's point, there is the economic value but there is also the democratic value and the privacy aspects. It all revolves around people's personal data, which is why I was so pleased to get the Data Protection Bill through Parliament earlier this year, introducing the GDPR into British law but also going beyond and really strengthening our data-protection arrangements and strengthening the powers of the Information Commissioner—updating her powers not just to fine but to investigate and interrogate and issue criminal sanctions.

That is all in the environment of protecting people's data and giving people power and rights over their data, as well as an appreciation, through education, of the value of that data. To some people, the value may be economic. Other people might just wish it to be kept private. But people need to be more aware of the data that companies and organisations hold on them.

Of course, people are now at liberty to make a subject data access request and find out what data an organisation holds on them. It is interesting to note that some American citizens are using our data protection laws to enforce their data rights against companies that are located in their jurisdiction, because of course in America at the moment there is nothing to compare with the data protection laws that respect the value of citizens' data here in the Europe.

Baroness McIntosh of Hudnall: I will come to the question I wanted to ask you, Minister, but on that particular point, it has been suggested, not just to us but more widely, that this whole business about people's data and the value and protection of it is severely undermined by the apparent fact that quite a number of people, particularly younger people, are far less concerned about the privacy of their data, how it is used and by whom than one would imagine—certainly a lot less than we are. Do you recognise that possibility and do you have any thoughts about it?

Margot James MP: I hesitate to generalise too much. You are absolutely right to say that people value their own privacy and data, online and offline, to varying degrees and that it might be interesting to do some research to find out what the demographics might look like. With young people, you are talking about people who have grown up with the internet and have never known anything else and have always had to accept a system whereby the major social media platforms through which they live their lives extract data—or have done to date—as the price for a so-called free service. With the awareness that I talked about earlier, people, including young people, are becoming cognisant of the fact that this is not free, in fact; that they are giving their data away and it has a value, as I was saying.

I attended a meeting of the British-Irish Council last week and the Scottish Government Minister present invited a young person who had been involved in the 5Rights initiative—I know Baroness Kidron has championed and developed that, for which I salute her—which was facilitated by the Scottish Government. It was very interesting. This young person gave a presentation to the meeting at which she said that she and various other young people involved had been really quite horrified at the extent of the extraction of data from them over which they had no prior knowledge and, until very recently, no control. I do not think we can necessarily break it down by age, but it is an interesting question and it would be fascinating to see a demographic analysis of attitudes to data and its value.

Baroness McIntosh of Hudnall: Indeed. Of course we should not generalise, but it is clear that attitudes to privacy, for example, are changing—for good or ill, I do not say.

Margot James MP: Yes, and people's awareness is changing and improving. Some people might welcome not being charged for the services—they are perfectly at liberty to do so—and they might be quite ready to give away data and so forth.

But it is not just the extraction and sale of data. There is another aspect to this, which is even less acceptable in my opinion: the processing of that data and the use of it in various opaque settings. I go back to the earlier discussion about democracy and the impact on people's voting behaviour. We are now in an environment where vast amounts of analysis can be made about a person based on information readily available to an internet platform about their browsing habits, their shopping history, where they live—all sorts of things. It is when that microdata is then used to target them in a way that does not have their consent and of which they are often unaware that it becomes very worrying.

Pricing is a key issue—going back to our airline discussion—such as the pricing of various utility providers. There is no doubt that that microtargeting and the amount of information now available to companies about people can result in those companies operating a differential charging system for their services, whether it is energy or telecoms or whatever. People who the company thinks are not likely to leave get charged more, and all this is going on with no transparency. That is what is so concerning.

Q193 **Baroness McIntosh of Hudnall:** Indeed, and that can also be used to exclude people from accessing services, which is another very big issue.

This leads directly to the question that I was supposed to ask you—sorry—which goes to the point of fairness and transparency, upon which you have laid great emphasis, quite rightly, both today and in the evidence that you sent us. It is pretty clear that it ought to be possible to design systems that are inherently ethical, transparent and fair.

A world of technology that can do everything that we can see it can do could certainly do that if it were minded to, but it is probably not minded to. It has been suggested to us that it is unlikely that design will naturally evolve to become ethical and transparent if the people who are doing the designing are left to themselves.

The question is therefore, first, what principles should determine what we mean by “ethical by design”. Secondly, and perhaps more importantly, because I know you have got to the principles, how do you then enforce them when it comes to applying pressure? Where will that enforcement come from? This takes us back to the regulation point.

Margot James MP: Ethics are very difficult to enforce, are they not? You want an environment where companies are incentivised and their motives and algorithms are aligned with the public good and a higher ethical standard. That is the ideal.

I share your concern that just leaving things to evolve might not lead us to that end state, which is why we have established the Centre for Data Ethics and Innovation. We expect considerable work and progress on these issues from that body. Once it has completed its first year of work, we will be closer to assessing the contribution it is likely to make in the long term.

I have high hopes for it as an organisation. It will ultimately be on a statutory footing and independent of government, and it has the potential to influence the development of technology very much for the good in the long term. We mentioned earlier the Center for Humane Technology; it has a similar remit.

It is good that these organisations are now putting their heads above the parapet and contributing to debate. There are already differences in behaviour when you look at different technology companies. There will be companies that want, in their DNA, to live up to high ethical standards.

When I worked in the pharmaceutical industry before I went into politics, there was a company, Merck, that was voted Fortune 100’s most admired American company year after year. The philosophy of the company's founder was that if you put the interests of the patients first, the profits will follow.

I believe in that as a principle of corporate governance, and I do not wish to imply in my evidence that technology companies are not capable of working all of this out for themselves and applying those high standards. That is what we want to see. However, I do agree that we cannot rely solely on corporate good citizenship, given the scale of the problem that we, and I am sure your Committee, have identified.

Baroness McIntosh of Hudnall: May I press you a little on that? It is interesting that you have pointed to the pharmaceutical industry, where there is clearly a huge potential for good and an enormous potential for harm. They may not be absolutely equal, but they are certainly close.

In the world of technology, and potential harms from technology, apart from issues where there is clear illegality, at the moment it is still up to the person or people who have experienced the harm to initiate the complaint, or whatever process there is. It still relies on the end user stepping forward and saying, "I have suffered this harm. What redress may I now look for?" It is perfectly true that in some cases there will be redress, but, to follow your pharmaceutical company analogy, you cannot leave it to the patient to be dead before you identify the harm. There have to be intermediate steps to make it less likely that a patient will be dead.

Margot James MP: Of course. I agree.

Baroness McIntosh of Hudnall: So following your own analogy, do you imagine a regime as strict as the one that applies in the pharmaceutical industry eventually applying in the world of digital?

Margot James MP: I would have to give that thought.

On the question of whether we need a stricter regulatory regime, yes, we do. Whether it needs to be as strict as in the pharmaceutical industry is something I would have to reflect upon before giving you a yes/no answer.

Undoubtedly, there needs to be greater regulatory oversight. It should not be left to individuals. Individuals should have recourse, but even ensuring that this happens now under the current system would be progress. I think we probably all feel that more needs to be done.

I will quote from the ICO's report into political campaigning. What the Information Commissioner says could apply equally across many of the harms that we are discussing. She said in her report last week, "Whilst voluntary initiatives by the social media platforms are welcome, a self-regulatory approach will not guarantee consistency, rigour or … public confidence". I concur exactly.

Baroness McIntosh of Hudnall: May I leave you with one thought for when you consider this further, Minister? The pharmaceutical industry depends hugely on innovation. There has to be, does there not, a constant stream of innovation in order for the benefits of the pharmaceutical industry to be realised.

One thing that the big tech companies and others frequently say about regulation is, "If you regulate, you will stifle innovation". I simply leave that for you to think about.

Margot James MP: By the way, it might reassure you that I do not accept that argument at all.

Q194 **Baroness Benjamin:** First, I would like to thank you for the recent announcement of the £57 million Contestable Fund for children’s programmes. Hopefully, some of those programmes will talk about internet safety. We will keep our fingers crossed.

My question is about online crime, which is happening thick and fast. The police now have to deal with a huge amount of online crime, including terrorist activities, child exploitation and gross sexual abuse. A friend of mine recently lost £84,000 in a bank transfer to Holland. It is happening thick and fast.

Do you think that the resources, powers and expertise provided to the UK police forces are sufficient for the sheer scale and complexity of online crime? Secondly, what initiatives are the Government carrying out to improve the UK’s co-operation with international partners to combat online fraud?

Margot James MP: Thank you for your kind comments about the Contestable Fund. I know you played a huge part in getting that initiative on the books, so thank you.

I completely concur that online crime, fraud and some of the terrible examples that you just mentioned—sexual exploitation, and so forth—are a scourge and need to be tackled vigorously. The Home Office has made funding available to the police to enable specialist units to assess the threat and identify criminality where they see it. I might have to write to the Committee on the question of whether they have adequate resource, following consultation with my counterpart in the Home Office.

I sit on the Organised Crime Task Force as the Digital Minister, and I feel that, whatever resourcing we have, we are facing a tidal wave and, as I said earlier, it should not all be down to the public purse to identify this material and get it taken down. We should expect this of the technology companies. They have proved that they can do it with terrorist content, so we need to hold them to the same standards, certainly for child sexual exploitation and sexual abuse images. That side of things should be treated absolutely as seriously as terrorism. The fact that we are not there yet is a severe indictment of some of the platforms. So I do not think it should all be down to the public purse.

If we can get the regulation right and our expectations set accordingly, we may find that we have enough resource within policing. I cannot be precise in my answer. The Home Office has allocated funds. Resources are always finite. Whether it is enough depends partly on what we expect the companies themselves to do.

Baroness Benjamin: What about online banking? You are encouraged to go online, and more and more people are losing money when they make huge transfers, especially to banks abroad.

Margot James MP: It is an area in which people have to be on their guard. The amount of online fraud is extremely serious. *Which?* magazine did a survey of online fraud and found figures in the billions. Consumers need to get advice from their banks and make sure that they double-check everything before transferring any significant amount of money.

In part, I am hopeful that this is an area in which technology will assist the banks in helping to protect their customers better than they are at the moment.

Baroness Benjamin: On the question of co-operation, how is the UK working with our international partners?

Margot James MP: There is a great deal of international co-operation with all global organisations, banking and financial regulatory institutions and the European Union. The Government are working with a whole range of international partners. Like most aspects of digital harm, it is global in nature and scope. So the Government are working closely with other regulators around the world to try to reduce all this.

Baroness Benjamin: Finally, what financial and other resources will be available to the UK Council for Internet Safety?

Margot James MP: I will write to the Committee with an exact response on that. The Council for Internet Safety is being revamped. It has a new board and a new remit, but I will write to the Committee to confirm what the resourcing will be.

Baroness Benjamin: Fantastic. Thank you.

Baroness Kidron: It struck me, in that last exchange, that so many of the answers to the extreme are also answers to the quotidian. As you probably know, the WePROTECT technical board will report on Friday on what we think will help to curb the spread of images of child sexual exploitation.

Without pre-empting the answer, so many things come back to impact assessments, the harmonisation of rules, designed standards and so on. I am interested to know whether you see extreme harm and everyday harm in the same continuum, or whether we are always going to be pushed into dealing with each harm separately.

Margot James MP: To a certain extent, different harms require different solutions, but I do see a lot of these things as a continuum. You have the horrors of child abuse images online. You also have child sexual exploitation online. Most of the time it is connected, I suspect.

Then there is grooming, which is at the start of the scale. Grooming concerns me greatly, because it is increasing. It is very easy for an older predator to masquerade as a young teenager and get the confidence of a young person, perhaps a vulnerable young person, online. Because so many young people live their lives online, they do not find it odd to make friendships online with a view to meeting someone.

Speaking for myself perhaps, we might have a natural sense of caution that, if you live your life online and have never known any different, you perhaps do not have. So I think children require greater protection in this area than adults. To my mind, at the moment they are not getting it.

Baroness Kidron: May I just add to that continuum? We know that there is one more stage: oversharing, competitive popularity, competition and, of course, addiction. We have seen that you start with that cultural piece and it goes all the way through the line. That is what I meant.

Margot James MP: Yes. I answered your question more in relation to child sexual exploitation, but potential addiction is another area. As the Lord Chairman asked earlier, is it the technology? What is behind it? People of all generations have been tempted to show off, as children, as young people, sometimes even as older adults.

Baroness Kidron: I cannot think who you mean.

Margot James MP: The thing about technology, as always, is that it enables and exacerbates and can be so much of a young person’s day-to-day experience that it becomes a problem, whereas in the offline world it was much easier to contain.

Baroness Kidron: A vast proportion of sexualised images of young children are actually posted by themselves, their friends or companions. That has grown in this environment, so I am keen to note that that forms part of the continuum.

Margot James MP: Yes, indeed it does. Thank you.

Baroness Benjamin: We have not mentioned online gambling, which I feel we really need to discuss when we talk about addiction and young people. Many university students at the moment are addicted to online gambling, and gambling companies are targeting young people to gamble online. I would like to know how the Government see this and how we are dealing with it, especially in the case of young students, many of whom are committing suicide and having mental problems because of online gambling and addiction.

Margot James MP: We are looking at online gambling as part of our White Paper development. We recognise that the online environment can exacerbate somebody’s gambling instincts and that gambling is introduced in areas where it perhaps would not have occurred before. All these things conspire to create a bigger problem, which we are definitely addressing in the development of the White Paper. Later this year, I have a round-table consultation on gambling, problems online and what we should be doing about it.

Baroness Benjamin: Fantastic.

Q195 **Lord Gordon of Strathblane:** We now turn to a specific aspect of international regulation. It is amazing that we did not come to it earlier. Inevitably, it is Brexit. What opportunities does it provide, and what threats does Britain face from it?

Margot James MP: Online?

Lord Gordon of Strathblane: Absolutely. I was not looking for a general answer.

Margot James MP: No. Good. We could have been here quite a long time.

In this area, this is a very global phenomenon. It is not an area where one country can easily introduce measures to unilaterally deal with the problem in one territory. There are things that the Government are doing, can do and will do, but we will always be better enabled if we act as part of a more global effort. When I say “more global effort” I ought to add the caveat “by like-minded countries”, because there are countries with a very different attitude to the internet that we do not necessarily want to emulate.

I met with my French counterpart last week, and we discussed various measures that the UK Government are taking, such as the requirement for pornography sites to have robust age-verification systems in place to prove that someone is 18 or over. My French counterpart is very keen to know more; they are looking to do something similar in France. I have mentioned Germany, which I think is already taking more action legally than any other country in Europe, and the Australians have introduced measures.

I do not think that Brexit will affect the online safety agenda either positively or negatively, with one potential exception: data. At the moment, our data protection regime is aligned with the European Union's GDPR, and we anticipate data being an important part—I hope—of whatever deal the UK leaves the European Union under. Data is an important part of that, but we will need an adequacy decision.

Lord Gordon of Strathblane: Do you mean on taxation?

Margot James MP: Data flows are very important. Of the United Kingdom's data flows, 75% are within the single market, within the European Union. The figure for our trade in physical goods is, I think, slightly under 50%, but for data it is 75%. It is therefore very important that we get an adequacy decision when we leave the European Union.

We are fully confident of getting one, but there may be a time lag between the end of the implementation period and the embedding of whatever future framework the Government are able to negotiate. During that time, companies will have guidance from the ICO and the Government on alternative legal routes to the trade in data.

Lord Gordon of Strathblane: While obviously agreeing that anything that we do would be better if it were universally implemented, there is still quite a lot that we can do, and indeed take a lead in, in the hope that others will follow.

Margot James MP: Yes. I am sorry if my answer did not give that impression. I apologise for that. We are doing hugely important things in this country. We are setting the lead on age verification, with the institute for data ethics and our White Paper development. We are in the lead in a lot of these areas, and these measures will have an effect. Will they have a greater effect if they are deployed across borders? Yes, they will, but that is not to say that they will not have a very positive effect when done unilaterally.

Lord Gordon of Strathblane: You mentioned the distinction between services and goods, which prompts me to ask the obvious question. The service industries, including broadcasters, were very much encouraged by the Prime Minister's Mansion House speech, and therefore slightly taken aback when the Chequers agreement did not provide for any protection for the service industries. Were you equally disappointed?

Margot James MP: My main concern, which is somewhat beyond my brief, was the trade in manufactured goods. The Chequers proposals were very strong on staying true to our desire for frictionless trade at the borders. It is different for services. I am not saying that the sectors I represent are not disappointed—I am sure they are—but the problems and challenges that they face are of a different order from those faced by manufactured goods.

Lord Gordon of Strathblane: But services are far more important to this country than goods when it comes to straight value for money.

Margot James MP: It is true that the economic contribution of services in this country is absolutely the greater; it is probably 75% of GDP. But I gave the example of data transfers. There are ways around the challenge of leaving the European Union that will not be to the detriment of the technology industry and companies that wish to send data over borders. I am confident that we will get an adequacy decision and that we will therefore be able to trade data seamlessly between Britain and the rest of the European Union, once we have that adequacy decision. I do not think that the problems are the same as they are for the manufactured sector.

Lord Gordon of Strathblane: Yet some broadcasters have already left for Amsterdam.

Margot James MP: On broadcasting you are quite right. I was answering with regard to data. It is true that broadcasting is another subject. We had a very good arrangement under the audio-visual services directive. For anyone who is not cognisant of this, it means that if a company satisfies the standards of one regulator, it can broadcast across the whole European Union. Roughly a third of all content broadcast across the European Union originates here in the United Kingdom. That regulation has worked very favourably for the United Kingdom.

Lord Gordon of Strathblane: And the loss of it?

Margot James MP: The loss of it will be regrettable, certainly, but the industry is looking at reciprocity, and there is hope that it will be able to counter the worst effects of the loss of protection under that directive. Although some of the organisations you mention are establishing operations in other countries within the European Union, I do not think that any of them are thinking that they will have to move all their operations. As long as they have a significant presence within a regulated jurisdiction of the European Union, that will be adequate. I am not trying to say that it will be as good—it will not—but I think there are ways of protecting the sector that will ensure that it does not have a calamitous result.

Q196 **The Chairman:** Thank you. We have talked a lot about regulation. The other side of the coin is education. In our inquiry into children and the internet, we found a lot of organisations out there trying to do good things in schools, working with children to get them to understand their role in looking after their own online security. We have talked about some of the banking scams, and we have all seen things that people have done which seem to be remarkably stupid—basically giving away their money. Again, education has an important role. We found a lot of good work but very little co-ordination and we called on government to consider what could be done to ensure that all of this work being done across the piece by voluntary organisations, government and schools, was co-ordinated and more effective. Have you had an opportunity to look at that?

Margot James MP: That is really high on my agenda right now. There is a need for greater co-ordination. In part responding to that need, the Government established the Digital Skills Partnership, which I co-chair with the chief executive of Cisco. That is designed to bring the various elements of skills training and confidence boosting under one purview.

The other great thing that we are now doing is establishing local digital skills partnerships between schools, universities and industry in a locality. In the

West Country, there is the Heart of the South West Digital Skills Partnership. There is one in the north-west, in Lancashire. I hope to launch the West Midlands Digital Skills Partnership jointly with my Secretary of State and the Mayor for the West Midlands early next month. It is a live issue. You are quite right to point it out.

There is a lot going on. We do not want to step in and take things over or stop things, but we do want to co-ordinate and through that process, I hope, identify any gaps. We do not want duplication and gaps, and I am hopeful that the local digital skills partnerships will be able to address those things.

Skills and confidence are absolutely crucial to citizens being able to enjoy the benefits of new technology on a more equal footing. At the moment, there are a lot of people, not just children, who are disadvantaged by not having the confidence to go online. Some 20% of people with a registered disability have never been online. That is appalling. A high proportion of people over 65 lack confidence online. We want the benefits of technology to be shared across society, not for certain groups to benefit while other groups fall behind.

Baroness Benjamin: You mentioned the partners you are working with. One partner you might be interested in working with is called UKBlackTech. I do not know whether you have been involved with it, but it is doing a lot of things for young black people who do not feel connected with the world that we are creating, and trying to get more BAME kids to understand the technical, online world that they are part of but not part of. I suggest you get in touch with it.

Margot James MP: Thank you for mentioning that organisation. I had not come across it. It sounds excellent and definitely a group that we will consult.

The Chairman: Minister, thank you very much for the evidence that you have given us and for being open with us and discussing many of the issues that we are considering as we produce our report. We will be reporting in the new year. I hope on behalf of the Committee that this could be the beginning of a dialogue in this very important area of public policy, and that when we report and you respond to us you may come back and talk to us about the issues that emerge from our report.

Margot James MP: I would be delighted to do that. Thank you all once again for this very important inquiry. I hope that the timing enables us to read it and look at its recommendations as part of the final stages of the development of the White Paper. We seem to be working in concert on this, and what you have done here is very valuable. Thank you very much indeed.

The Chairman: Thank you and thank you for your time.

Margot James MP: Thank you.

Her Majesty’s Government – supplementary written evidence (IRN0124)

Follow-up letter to the Chairman from Margot James MP, Minister for Digital and the Creative Industries, Department for Digital, Culture, Media and Sport

Thank you for your invitation to give oral evidence to your Committee on Monday 12 November 2018. I enjoyed the discussion around the very important topic of internet regulation, with the variety of views that were brought to the table. I look forward to being able to consider your report as part of developing the Online Harms White Paper for publication in Winter 2018/19.

I am writing to answer a number of questions that were raised during the debate.

1) Scale of response to the Government consultation on the Internet Safety Strategy

Regarding the question raised by Baroness McIntosh of Hudnall about the scale of response to Government’s consultation on the Internet Safety Strategy Green Paper, we produced two versions of our online consultation survey - one for individuals and one for organisations. The survey for individuals included questions on both personal online experiences and our policy proposals, whereas the survey for organisations only included questions on our policy proposals. 528 individuals and 62 organisations responded to our survey. We published the government’s response to the Internet Safety Strategy Green Paper in May 2018. This provides details of the response to our public consultation.

I would also like to reassure the Committee that the Government’s consultation is only one element that will help to inform our decisions. Our evidence gathering process is much wider. My department is currently undertaking roundtable consultations with major stakeholders, including industry (both big tech companies and Small and Medium-sized Enterprises), civil society bodies, charities and regulators, to gather evidence, opinions and recommendations. My department regularly reviews the available literature to ensure that our policy development takes into account valuable and independent research, and we are also commissioning our own research on different aspects of Online Harms to address gaps in the evidence base.

2) Resources, powers and expertise provided to UK police forces

Regarding the question raised by Baroness Benjamin about the resources, powers and expertise provided to the UK police forces, this is primarily a matter for colleagues at the Home Office. The Home Office and DCMS agree that individuals offending online should be brought to justice and face the appropriate penalties for their crimes; and companies should work with law enforcement to ensure that crimes committed on their platforms are dealt with quickly and effectively. The Home Office is working with the police to better understand future police demand, what capabilities the police need to respond, and how efficiency and productivity can help improve services. The Chancellor recognised in his Budget speech that the police are under pressure from the changing nature of crime. He made clear that the Home Secretary would review police spending power and reform ahead of the 2019/20 police funding settlement.

The Government is committed to ensuring that the police have the resources they need to undertake their crucial work. At the 2018/19 police funding settlement, the Government recognised that demand on police from crimes reported to them has grown, shifting to more complex and resource intensive work such as child sexual exploitation and modern slavery. The Government increased total investment in the police by over £460m in 2018/19.

The Investigatory Powers Act 2016 permits law enforcement to use a number of investigatory capabilities to obtain communications and data about communications. It ensures that these powers and the safeguards that apply to them are clear and understandable. The Act restored capabilities that have been lost because of changes in the way people communicate and made investigatory powers fit for the digital age, for example, by creating a new statutory basis for the retention and acquisition of internet connection records (ICRs), a record of the internet services that a person or device has accessed.

I can also reassure the Committee that through the National Cyber Security Programme (NCSP), the Government invested over £100m under the 2010-15 parliament, and £80m since 2015, to bolster the law enforcement cyber crime response, developing a single, whole system approach at the national, regional and local level. This includes boosting National Crime Agency capabilities, increasing their ability to investigate the most serious cyber crime, continued investment in Regional Organised Crime Units (ROCUs) and creation of local units in all 43 Police Forces in England and Wales. The Home Office keeps the Computer Misuse Act, which defines offences and associated penalties for unauthorised access to and modification of computer systems, under regular review to ensure it keeps pace with the evolving threat and law enforcement agencies have the powers they need. This was last revised in 2015, to include new offences relating to hacking which causes serious damage or pose threat to life.

The Home Office is also investing £36m over the 5 years from 2015/16 to 2020/21 in the Action Fraud service. The City of London Police launched an improved service on 6 October 2018, based on an updated IT analytics engine allowing the Police, private and public sector organisations, and the public to quickly and easily report fraud and cyber crime. Police Forces will be able to access intelligence faster with information and analytics they receive from Action Fraud being more comprehensive and accessible.

3) Financial and other resources available to UKCIS

Regarding the question raised by Baroness Benjamin about financial and other resources that will be available to the UK Council for Internet Safety (UKCIS), the UK Council for Internet Safety is a voluntary, non-statutory body, and does not receive any discrete funding. UKCIS members volunteer their time to work on collaborative projects in a number of areas agreed by the UKCIS Executive Board, including online harms guidance for schools, and the interrogation and dissemination of evidence of online harms. UKCIS is supported by a small Secretariat team at the Department for Digital, Culture, Media and Sport (DCMS).

I am copying this letter to all members of the Lords Committee on Communications and Lord Ashton.

3 December 2018

Professor Derek McAuley, Dr Ansgar Koene and Dr Lachlan Urquhart, Horizon Digital Economy Research Institute, University of Nottingham – written evidence (IRN0038)

Horizon[826] is a Research Institute at The University of Nottingham and a Research Hub within the RCUK Digital Economy programme[827]. Horizon brings together researchers from a broad range of disciplines to investigate the opportunities and challenges arising from the increased use of digital technology in our everyday lives. Prof. McAuley is Director of Horizon and was principal investigator on the ESRC funded CaSMa[828] project (Citizen-centric approaches to Social Media analysis) to promote ways for individuals to control their data and online privacy and the EPSRC funded UnBias[829] (Emancipating Users Against Algorithmic Biases for a Trusted Digital Economy) project for raising user awareness and agency when using algorithmic services. Dr Koene led the research of the CaSMa and UnBias projects. Dr Urquhart is a research fellow in IT law, researching challenges and solutions to regulating emerging technologies.

Questions

1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

When considering regulation for the internet it is important to make a distinction between the question of 'regulating the internet infrastructure', i.e. the underlying communications infrastructure, vs. 'regulating services that are built on the internet' (e.g. media and commerce platforms and services).

Regarding the internet infrastructure, the focus should be on *facilitation of access*, which includes regulator support for an appropriate concept of Net Neutrality – that is, internet communications service providers should not be permitted to discriminate against specific classes of traffic or users in normal operations.

For services built on the internet, often referred to as platforms, the primary focus needs to be on appropriate application of existing offline regulation to online service providers, and where it is deemed inadequate, updating that regulation to deal with the gap.

Regulation (and application of regulation) should focus on the function that is provided, not the medium through which it is delivered. Thus, a business that facilitates chauffeured private car hire services should be regulated the same regardless of whether the service is provided via an app (e.g. Uber), a phone call, or telex. Indeed, much existing legislation has been applied in this way despite the repeated complaints from some service providers that the use of the Internet should in some way exempt them from all existing legislation.

[826] http://www.horizon.ac.uk
[827] https://epsrc.ukri.org/research/ourportfolio/themes/digitaleconomy/
[828] http://casma.wp.horizon.ac.uk
[829] http://unbias.wp.horizon.ac.uk

A key challenge in regulating these services built on the internet is the international nature of such service delivery, which can cause confusion regarding jurisdiction, and subsequently the problem of how those affected can seek redress. This is a fundamental issue that has been recognized and addressed in the GDPR by focusing on where the impact of processing occurs, i.e. the location of the data subject. So generally, it is the case that services targeted at specific jurisdictions through localization, whether through language or tailored local content, and generating revenue from such localization should be required to obey the regulation within that jurisdiction.

As an example, the fact that online platforms are increasingly becoming the information gateway for people, especially younger generations who get much of their news from online platforms via mobile devices, raises social and political concerns similar to traditional news media. Concerns about media empires with too much dominance in newspapers or TV coverage, should equally apply to online platforms where it is now common for a single provider to dominate a service sector (Facebook for social networks, Google for search). As shown by Facebook's own study (2012 US elections impact on likelihood to cast a vote[830]), they have the power to influence voting behaviour.

In summary, given the broad uses of internet technologies, and the wide range of legislation that already applies, a specific internet regulation can only address those elements that are specific to the internet technologies and not apply to all the myriad uses to which such technology can be put. Much of this is already covered by more specific regulation, which should be more rigorously enforced and updated as necessary.

2. *What should the legal liability of online platforms be for the content that they host?*

It is necessary to differentiate between the many possible different roles of online platforms, as examples consider platforms:

- Engaging in, or facilitating, open or broadcast communication (e.g. YouTube);
- Offering private person to person, or closed group communication (e.g. WhatsApp);
- Performing personalization of content (e.g. Facebook).

The test for legal liability must be based on an independent assessment of the role that the platform takes, noting that a platform may simultaneously take on multiple roles – for example, many platforms offer both person to person private communications while also engaging in algorithmic personalized editorial control of third party contributed broadcast content.

A service provider operating as a broadcaster of content, however sourced, should be held to regulations concerning broadcasters.

Platforms that provide private communication (whether encrypted or not) between closed groups should be regulated as such in this role, directly in parallel with

[830] https://www.nature.com/articles/nature11421

traditional telephone communication. So, they should not be held accountable for content in such private communications, but neither should they be permitted to process it other than in a manner essential to convey it. Hence, a company that processes the content of email to target adverts should not simultaneously be permitted to claim merely to be a "communications provider".

Service personalization is frequently used with the claim that it improves the customer experience, and this frequently involves filtering/recommending the products/services/information the customer is presented with. However, the algorithms are of course actually driven to optimize revenue, and as these algorithms become increasingly complex and adaptive, platform providers themselves may not be able to guarantee that they are compliant with regulations - for example, the personalization may in fact be based on illegal profiling using gender, ethnicity or a myriad of other types of sensitive personal information. However, such algorithmic content moderation is still an editorial engagement with content, even though it does not involve direct human intervention. The platform provider controls how the algorithm is set up, what its prioritization metrics are, and should be held accountable.

In-site linked advertising can cause specific problems, especially for sites that are meant to be child-friendly (by using child targeted content filtering) because the advertising content hosted on websites is usually under the control of a third-party ad delivery service (e.g. AdSense), which run real time auctions to determine which advert to show. Various ad delivery services do include customization options that allow the site owners to tune the type of ads they allow on their site, but often these settings are not used or fail to match the age appropriateness of the site content. Service providers should be held accountable for such contracted third party content.

In general, a broad sweeping internet regulation cannot possibly capture all the roles that service providers take on with regards to content.

3. How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

Noting para. 11, internet infrastructure providers, and "over the top" platforms while performing the role of providing private closed group communications services, should not be required, or indeed permitted, to moderate content.

Many platforms currently claim the protections afforded to such communications service providers, even when content is made publicly available, and prefer not to moderate content in advance, but rely on user take down requests for illegal or inappropriate content. However, such take down requests include many frivolous and malicious requests, sometimes aiming simply to censor content which the person reporting disagrees with. Hence it is only right that the moderation process should be one of transparent arbitration, which would be greatly helped by the wide adoption of a common code of practice and common processes.

4. What role should users play in establishing and maintaining online community standards for content and behaviour?

Some online communities are defined by their community standards and decide what is appropriate – indeed many platforms exist to support such community interaction. However, the handling of illegal content is a matter for law not community opinion, and the appropriate role of the community is simply to flag suspected content into a transparent arbitration process.

5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

Some platforms provide the means to label content as "adult", which is a somewhat blunt distinction – in film, TV and computer gaming[831], age labelling and controls are more nuanced and online service providers could use similar, rich content labelling schemes – even better if adopted as international standards and capable of being automatically applied through appropriate browser settings.

In our research, participants of our "Youth Juries" suggested the creation of peer-group advice services to support both parents and children with practical advice concerning online security based on personal experiences - online platforms could be encouraged to support such initiatives or at least sign post them for users.

Related to freedoms of expression and information, the previous comments on moderation apply.

In addition, the previously discussed data-driven personalization can result in what has been referred to as a "filter bubble" where the personalization algorithms limit information visibility, hence imposing an unintended block to freedom of information – again we need to call for appropriate transparency as to this profiling, and the right and ability to remove it.

6. What information should online platforms provide to users about the use of their personal data?

This is covered extensively in the EU GDPR and the associated UK Data Protection Bill; what is now required is rigorous enforcement by the Information Commissioner. However, public engagement with, and understanding of, such legislation is poor.

A key element of modern data protection regulation is the role of the technologists, as non-state actors, in regulation through concepts like privacy by design and default (e.g. in Article 25 GDPR). How they design the technology has regulatory implications and mediates how users behave. However, it is also important to go beyond Privacy by Design as a compliance tool, to a mechanism for dialogue with citizens about what values they want embedded in technology, and how. It can be a medium for bringing wider human values into design from the beginning. Such participatory design would greatly aid wider public understanding of how their data is used.

7. In what ways should online platforms be more transparent about their business practices – for example in their use of algorithms?

[831] Pan European Game Information http://pegi.info

Technologists like to think of their algorithms as neutral, but the modern class of goal driven big data algorithms will reflect any biases in the selection of data types selected for processing as well as biases present in the training data itself. So, yes, online platforms should be more transparent about how they work. They should provide clearer insight into the kind of data they collect and process about users, including behaviour and activity tracking, as outlined in the House of Commons Science and Technology Committee report on Responsible Use of Data (Fourth Report of Session 2014-15).

Service personalization is frequently used with the claim that it improves the customer experience, and this frequently involves filtering/recommending the products/services/information the customer is presented with. However, the algorithms are of course actually driven to optimize revenue, and as these algorithms become increasingly complex and adaptive, platform providers themselves may not be able to guarantee that they are compliant with regulations - for example, the personalization may in fact be based on illegal profiling using gender, ethnicity or a myriad of other types of sensitive personal information. However, such algorithmic content moderation is still an editorial engagement with content, even though it does not involve direct human intervention. The platform provider controls how the algorithm is set up, what its prioritization metrics are, and should be held accountable.

For many online platforms the default business model has become the 'freemium'/free to use model that is supported by advertising revenue. While the obvious side of the advertising revenue are the ads that are shown on an online platform, a second source of income is often the sale of platform user behaviour statistics. Data are commonly gathered through multiple sources, including: storing of the information that is posted to the platform (e.g. product reviews), tracking of user behaviour on the site (tracking-cookies track behaviours like, where the users has clicked on a site and the amount of time between clicks), purchasing of data about behaviour/interest of demographic classes of users. The data is used to sell targeted ad space to advertisers and to feed into the filtering/recommender algorithms that 'personalize' the user experience. Users typically have very little control over any of this data collection. Privacy settings on sites like Facebook primarily stipulate how information is shared between users, not how the platform provider gathers and uses the data. Terms & Conditions of online platforms are usually formulated to give maximum freedom to the platform provider to use the data as they wish. For example T&Cs often include vague, broad-stroke, clauses such as 'data may be used for research purposes', where the research question is not specified to the user. Users usually have no options to control how their data is used, if they want to use the services, or even just part of the services, of the platform provider, they have to consent to handing over full control of their data to the platform. Various platforms do provide users with comprehensive access to the content that the user contributed to the platform, such as a download of the posts that were made to G+, but do not provide access to the tracking data that was collected about the user.

8. What is the impact of the dominance of a small number of online platforms in certain online markets?

The internet was founded on open standards and interoperable federated services. This offered a landscape for competitive innovation that is now being restricted by isolated "walled gardens" and for the large players, aggressive acquisitions strategies that remove competition before it arises. As noted in the House of Lords inquiry into Online Platforms, such acquisitions do not satisfy the criteria required to be subject to scrutiny by the Competitions and Market Authority (or equivalent elsewhere), and this could usefully be reviewed.

9. What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

International coordinated regulation is required in order to have impact, and specifically on large US corporations which have emerged within the US's specific regulatory framework. In this regard the EU is an important player, and the UK has been an important contributor to the EU position, whereas the UK will in future be a minor voice unless it continues to coordinate and support EU action in this area.

3 May 2018

Mark Stephens CBE, Partner, Howard Kennedy LLP and Jenny Afia, Partner, Schillings – oral evidence (QQ 58-70)

Tuesday 19 June 2018

Watch the meeting

Members present: Lord Gilbert of Panteg (Chairman); Lord Allen of Kensington; Baroness Bertin; Baroness Bonham-Carter of Yarnbury; The Lord Bishop of Chelmsford; Viscount Colville of Culross; Lord Goodlad; Lord Gordon of Strathblane; Baroness Kidron; Baroness McIntosh of Hudnall; Baroness Quin.

Evidence Session No. 8 Heard in Public Questions 58 - 70

Examination of Witnesses

Jenny Afia, Partner, Schillings; Mark Stephens CBE, Partner, Howard Kennedy LLP.

Q58 **The Chairman:** Can I welcome our witnesses to this session of our inquiry into the regulation of the internet? I will ask our witnesses to introduce themselves in a moment. Just so they are aware, the session today is being broadcast online and a transcript will be taken. I am very grateful to our witnesses for coming along and giving us evidence.

Could I ask Jenny Afia and Mark Stephens briefly to introduce themselves and tell us a bit about their background, and in so doing, just so we know where they come from on this very broad subject, tell us whether there is a need to introduce a new regulatory framework for the internet and the wider digital economy? If so, what form should it take? Should it be largely imposed regulation, self-regulation or co-regulation? Is there a need for a new body to establish that regulation or to co-ordinate the work of existing regulators in the field?

Jenny Afia: Good afternoon. I am a partner at the law firm Schillings, where we specialise in safeguarding privacy. Our clients include some of the world’s most successful people. Even for them, with all their resources, trying to have information removed from the internet can be very distressing and very difficult. I really worry what the experience is like for people with fewer resources, most particularly children. I have worked with the Children’s Commissioner on her digital task force and I have provided support to the 5Rights Foundation led by Lady Kidron. Most recently, we co-authored a report entitled *Disrupted Childhood*, which looked at the impact of persuasive design strategies on children’s mental and physical health.

The first project I did for the 5Rights Foundation, which is relevant to your question, entailed a review of the existing legislation at the time to see what support there was for the 5Rights framework. This was in 2014 and 2015. My conclusion then was that we did not need new laws; we needed better application of the laws and better awareness of what the laws were. If you ask me now whether we need a new regulatory framework, I still think we probably do not need new laws, although had you asked me about a year ago, in between the two questions, I would have said yes. Since then we have had the GDPR, with its emphasis on privacy by design; we have had the Data Protection Act with the age-appropriate design code. I know there are several reviews going on, looking into the issues of artificial intelligence, and there is the Law Commission review.

I have also seen how industry has improved its standards. For example, there is the new operating software coming out by Apple in the autumn. Some of the changes Instagram has made, for instance its attempts to tackle bullying, have been really impressive. At the moment, we have sufficient regulation. The problem is that it is all a little reactive and piecemeal, and I do not know what lies ahead because I do not have sufficient technical expertise, and neither do my clients, to see what is coming down the line. If we are happy with this reactive model that does not seem to encompass a root-and-branch approach to the internet, at the moment we do not need a new regulatory framework.

***Mark Stephens*:** Thank you for inviting me here today. My name is Mark Stephens. I am a partner in the London law firm of Howard Kennedy. Perhaps also relevantly, I was the founding chair of the Internet Watch Foundation back in 1996—almost before the internet was born and certainly before Facebook, Google, Twitter and all the others—with its avowed intent to remove paedophile material from the internet. I have been working as an adviser with the UN counter-terrorism executive directorate, and we hold meetings on extremist content around the world. I work with ICT4Peace and, last but not least, I am the independent chair of the Global Network Initiative, which is also a multi-stakeholder initiative that brings together academics; ethical investors such as the Church of Sweden and their ethical investment funds; corporates and NGOs that are informed in this space; and people from the ICT sector.

You asked about the need for a regulatory framework. The best place to start with this is that there is a need to look at that word "regulation", because it can mean a wide spectrum of arrangements between the relevant actors. At one end of the scale it can include voluntary commitments by companies, and at the other end it can mean binding laws with government enforcement. Between those poles lies a range of possible arrangements which exhibit various degrees of flexibility, transparency and accountability. I would draw attention to the fact that the Internet Watch Foundation was founded specifically to deal with one of the most pernicious problems at the time, namely paedophile material. I think it can be said to have been a success in that space.

In relation to the *Internet Safety Strategy* Green Paper that Karen Bradley published, there were some interesting things. There were three things that she really focused on. First, what is unacceptable offline should also be unacceptable online. That gets a tick; we all agree with that. All users should be empowered to manage their online risks and stay safe. That gets a tick; we all agree with that. Technology companies have a responsibility to their users. That gets a tick; we would all agree with that, although the real question there is to what extent they have that obligation, how they show they are doing it and how they empower people. I would, though, add a fourth: if there is to be legislation, it should be clear and unambiguous so that people and companies may properly identify and regulate their behaviours.

Yesterday, I was in Germany, where we were looking at the NetzDG legislation, and I will perhaps come back to that in a minute. But what is interesting is that technology companies have already acknowledged that they have a responsibility in this space to their users. They are using transparency reports; they are taking on hash sharing; and they are policing their own community standards, which invariably stand well within the bounds of the law. Therefore, the principled approach is to identify a lacuna in the existing law or some pressing social need, and then, if there is a pressing social need, to find a way in which we ought to proportionately fill it.

A note of caution here is that legislation can often be slow and cumbersome; Jenny was adverting to that a moment ago. In this fast space, private responses may well be more potent than government ones because they can respond more swiftly and in a targeted way. One of the questions we have to ask ourselves is this: is there a way of encouraging those companies to perform in that middle space without formal regulation but perhaps within a framework? One framework I was looking at, and have been looking at for some time, is that of the Ruggie principles, the UN guiding principles on business and human rights, which apply to companies, alongside their obligations to report and ensure compliance with human rights and the law more generally.

At this point I have concluded that, certainly looking at the NetzDG legislation, it is not working very well and it is not a lesson we would be wise to follow. It is interesting that you have David Kaye, the UN special rapporteur on free speech, and the German data protection officer—their version of the Information Commissioner—criticising the law. You have seven out of 10 German law experts in the Bundestag criticising the law, as well as really top legal German academics concluding that the law does not achieve its objective, promotes overbroad blocking and has passed the responsibility to prosecute criminal offences from the Government to the private sector, of course with a chilling effect on private speech.

I am concluding, Chairman. This is all against the backdrop that two FDP parliamentarians—those are the liberals to us here; I am sure you all knew that but I did not—last week in Cologne applied to have the law struck down. It does not even look like it will last a whole year. That would not be a good place to be in. It is interesting that the renowned German legal scholar Professor Gerald Spindler has noted that NetzDG is likely to breach EU data legislation, particularly the e-commerce directive, the GDPR, the e-privacy directive and other legislation. We have to think about how those intertwine at the moment.

The Chairman: Thank you both for very helpful opening contributions.

Q59 **Lord Gordon of Strathblane:** This is a question, perhaps first of all, for Mark Stephens, as you were the founding chair of the Internet Watch Foundation. The present CEO gave evidence a few weeks back and made a fairly passionate plea: "Our plea is that our self-regulatory approach is acknowledged as working"; it "is not broken and does not need fixing". Is that self-regulatory approach unique to that particular segment of the problem or could it be expanded?

***Mark Stephens*:** First, IWF is not self-regulatory. It is paid for by the industry, but it is actually a multi-stakeholder environment. That would be a more appropriate response. It has child protection people involved in it—they are very important, and I mean people at Childline and other organisations—as well as the industry. It recognised that there needed to be a partnership between the people who were seeking an outcome, which in fact was everybody. Everybody is looking for the same outcome. They all want to remove paedophile material, and they want to work together and draw on the expertise around the table to achieve that in the most efficacious way.

If you look at the Global Network Initiative, it does the same thing: it brings together different kinds of expertise. The challenge is that the problems are disparate. Therefore, I am not convinced that having one umbrella organisation actually produces the outcome you want. The GNI is about as close as it gets, because it is multinational. It has all the major ICT companies from Europe, from BT and Vodafone right the way through to Telia, and it then has the big American platforms such as Google, Microsoft and Facebook, along with those other independent experts who hold them to account. It is important; it works on its own terms. But I am not sure there is a broader role at this particular point in time.

***Jenny Afia*:** I do not believe that, on several issues, self-regulation has worked with the internet to date. My biggest concern is that children’s best interests have been ignored probably because of the utopian vision that all internet users would be treated equally and, de facto, if everyone is treated the same, children are treated in the same way as adults. That has led to very significant issues, but I hope those issues are going to be addressed by the age-appropriate design code. I do not believe self-regulation has worked at all. Children’s best interests have been sacrificed for commercial gain. But I am optimistic that the situation is being addressed, on a piecemeal basis.

Lord Gordon of Strathblane: Would you agree that it has worked in the case of the Internet Watch Foundation? I accept the caveat that it is not entirely self-regulatory.

***Jenny Afia*:** People who know more about it than I do hold it up as the industry standard. I really do not have any more to add.

***Mark Stephens*:** That is very kind of you.

Lord Gordon of Strathblane: I was wondering whether there might be a way forward through protecting the individual citizen rather than looking at the regulation of internet companies. Is the idea of an internet Bill of Rights a feasible option?

***Mark Stephens*:** You have to go at it with this principled approach. The way I have looked at it is to ask, “What are the basic rights we have as citizens?” I am not sure an internet Bill of Rights gives us anything more than we already have. Again, I come back to the UN guiding principles on business and human rights, which are grossly overlooked by many companies that have voluntarily taken them on. They impose an international law obligation on companies, particularly transnational companies, to behave ethically and appropriately in accordance with the law. That is where the problems lie.

One challenge in much of what Jenny was referring to, particularly around children, with which we would all agree, is that the publishers are often the problem and not the people who are conveying the information. We see that whether we are dealing with extremist content or vulnerable groups within society.

Jenny Afia**:** I am not keen on the idea of an internet Bill of Rights, because rights should apply irrespective of the environment. This is not how children understand their worlds. The distinction between the offline and online world will fairly soon become antiquated, so the emphasis should be on universal and fundamental human rights.

Q60 **Viscount Colville of Culross:** Good afternoon. We have heard from a number of witnesses that internet intermediaries should be much more liable legally for the content they have on them. The ICO, for instance, has said they "produce content, filter what individuals view and in some cases micro-target individuals with advertising". Should the safe harbour protections in the EU e-commerce directive be amended or abolished altogether? In that case, is there something else that could replace it to try to increase that liability? Mark, you talked about the German NetzDG law going far too far. Is there something in between that would allow us to give more liability to the internet intermediaries?

Mark Stephens**:** One of the flaws of the NetzDG law, to be completely candid about it, is that it covers 22 different offences under the German criminal code, and that just lends itself to a lack of clarity and a clash with other areas of the law.

Going back to your question, it helps. The safe harbour has been quite helpful in this space. I have been working with the UN counter-terrorism executive directorate, and we have had some security briefings. There are obviously some things I cannot say in open session, but there are some quite important things I can share. One is that jihadi extremists who create original content are numbered at about 70. We know where they are located by reference to the cell towers through which they upload material. That original content is amplified by about 200 to 250 further individuals, and then it spreads its disease from there. The interesting thing is that the jihadis could migrate to smaller platforms and perhaps areas where regulation was less thorough, but they do not do that. Intercepts tell us that they want to be on the larger platforms, because they feel they have a greater reach and, as a consequence, they complain internally about how quickly their accounts are being taken down. It is not just the individual posts and the videos, but the whole account is being taken down. A game of whack-a-mole is being played.

For that reason, we are seeing the platforms taking urgent action, and we need to encourage them to do that. As a consequence of that, giving intermediary liability is not very helpful. I go back to the days of paedophilia on the internet. The Internet Watch Foundation was born of the fact that the police wanted to prosecute internet companies for "hosting" material they did not even know they had. It was recognised and conceived, I think very wisely, that a much broader partnership in the public good was to not prosecute, to give them that immunity and to allow them to co-operate with law enforcement and report all the material they find, so those people who share that kind of disgraceful material can be found.

We have decided, for good and decent reasons, not to turn the cell towers off for the individuals where we know where they are located, partly because we are going to get good intelligence from them, and we do. It would be wrong to burden the platforms with the obligation of not only playing whack-a-mole, which they are doing as best they can, but also with some measure of liability. That is the opening concern I have in relation to starting to down that route.

Jenny Afia**:** I like the concept in principle. From my sense of justice, it makes sense to me. My experience on the ground is that content is not removed quickly enough. I am also told by social media companies that efforts are being made to change that, and I very much hope that is the case. Day to day, our experience is that it takes a long time and a lot of banging on doors or knocking on algorithms to have content removed.

Viscount Colville of Culross: Should we have a duty of care established by statute to stop online harm? If so, how might that code work?

Jenny Afia**:** I am interested in the idea on the basis that, if we draw an analogy with the physical world, we have the concept of a duty of care. There is a duty of care to take steps to avoid harm in the workplace, in public spaces, in parks and when you build homes. To the point I made earlier about there no longer being a distinction between the online and offline worlds, it would make sense to extend that duty of care in principle. It would still be worth, particularly given Mark's point about unintended consequences, identifying the harms that are not currently being addressed. If we are satisfied that there is a lacuna, in principle the idea is quite appealing.

Mark Stephens**:** One of the challenges around a duty of care is that it requires you to be aware of the problem you have. Let us take hate speech for a moment. The platforms are all aware that they have the problem, in line with their obligations under the Ruggie principles, the UN guiding principles on business and human rights. They are taking actions. We can argue about whether it is enough, but they are taking actions. As a consequence, I wonder what we get from ratcheting up the obligations on them. They have a view internally, and it is quite clear to me that they do not want this material on their platforms, because it falls in breach of their own community standards. We had a rather bizarre situation of a case in Berlin a few months ago, in which it was determined that Facebook had taken down something under the NetzDG law that was lawful, but Facebook still kept it down on the grounds that it was in breach of its own community standards. We are likely to get into problems with this.

Q61 **The Lord Bishop of Chelmsford:** I wonder if we can keep going with the topic we have just come on to, the moderation of content. Jenny, certainly in your written submission, this is something you were particularly writing about. I have two questions, really. Are the processes used by the online platforms to moderate online content fair, effective and transparent? Particularly, what processes should be implemented for individuals or organisations that wish to reverse decisions? Who should be responsible for that? I want to hear from both of you but, Jenny, given what you have been saying, it would be great to hear what you think could or should be done.

Jenny Afia**:** The processes used to moderate content are not that fair currently, because they do not even seem to comply with their own terms of use. We have seen a few examples of this. Recently, we had a female client, and somebody on Twitter and then posting on YouTube was calling for her to be genitally mutilated. Both YouTube and Twitter said that did not contravene their terms. We have had photos identifying the home of a client, a high-profile businessman, with frightening accuracy. Those photos were published on YouTube, and we were told they did not violate privacy policies. We have various examples where content is not removed that, on the face of their own community guidelines, would seem to contravene them, which does not feel fair.

Are the processes effective? They are effective sometimes or often, but not often enough. It is concerning. It is horrid. I hate getting internet cases, and there are loads of them, because you do not have a degree of confidence that you can help a client even though the law is on the client's side. The processes are not that effective and they are definitely not transparent. You do not know if a human has made a decision on your complaint or it has just been determined by an algorithm. It feels like there should be a process for internet users who want to reverse decisions to moderate content, short of having to bring litigation.

I know Australia has the e-safety commissioner model, which is a form of ombudsman that you can take complaints to. I asked some Australian practitioners about their experience of it, and it has been fairly limited so far, so I do not feel that qualified to say how effective it has been. But it feels like it would better protect both the right to privacy and the right to freedom of expression if there was another body in place that could help determine complaints.

The Lord Bishop of Chelmsford: I have a supplementary, but I would like to hear what Mark has to say first.

***Mark Stephens*:** I will try to keep it as brief as I can. Content moderation across platforms varies quite considerably. That is more so because companies are at different stages of evolution. I would exhort the Committee to think that the most profitable way forward is perhaps to focus on methods of reporting. How do you get to the page to report it? How do you know it is being responded to? If you were going to a regulator, whether it was self-regulation or statutory regulation, you would expect a certain degree of outcomes; you would expect progress reports. You would expect all those things that could helpfully be expected of them.

It is interesting to note, from my experience, that European ICT companies have more experience in transparency reporting than those in the US. They are rushing to catch up, but a good example is that Google will allow anyone in the company, or indeed outside, to put forward suggestions as to how reporting can be improved. For example, to Jenny's point about not knowing whether it is an algorithm or a human, in fact everything is reviewed by a human. The problem is that humans are fallible, as are algorithms, I suspect.

This is the challenge here: how do you direct the travel towards a greater amount of takedown? The best work I could refer to you that I have seen is the Berkman Klein Center's report *Account Deactivation and Content Removal*, from 2011. I have not seen anything subsequent to that, but it was pretty comprehensive and it was well done. The gap in this part is that each company has its own transparency reporting; you cannot read across from one to the other. We should be able to make that read-across, to determine who the best actors are, where the industry's gold standard is and where the suboptimal players are.

The Lord Bishop of Chelmsford: Human fallibility is my specialist subject. This may be the naive question to end all naive questions. There seems to be this debate going on about the need for freedom of expression and how we moderate and regulate content. But part of me—we have heard this from other witnesses—wondered whether it could work the other way. The algorithms could be geared not to wait until the content comes up and then ask, "Could you take it down?" Could the algorithms work much harder to stop the content going up in the first place? Then you appeal to have it put up if a mistake has clearly been made. Is that a completely ridiculous thing to suggest?

***Jenny Afia*:** No, it is not. People at Instagram, for example, are working on that at the moment. They have introduced what they call bullying filters. They have identified certain words that are so obviously offensive they cannot even be uploaded. That goes to your point about that really early intervention stage. There is a problem, they explained to me, given where the technology is at the moment. Suppose you had a scenario where a child was bullied at school all day and they were being called a dog all day. They get home and they receive one message via social media that says "woof". The system cannot yet identify how distressing that would be for the child, but I believe they are trying to work on precisely those proactive measures. I hope that will set the market standard.

***Mark Stephens*:** It is important to say that those things are coming and we are going to see design building them in to address these issues, as you say Instagram is doing. But there is also a need for a review. If somebody has something taken down and we effectively have monopolistic platforms, how does somebody get redress in those circumstances? There has to be some kind of ombudsman. If you look at newspapers, for example, they have independent ombudsmen, but we see them in all sorts of sectors. I see no reason why this ICT sector should not have an independent ombudsman who could address complaints where people think their material has been wrongly taken down.

Q62 **Baroness Kidron:** I am just going to declare my interest, in that I know Jenny Afia very well. Mark, can I ask you a tiny question about whether you think there is a role for consumer law in this? I was interested in what you were saying about universal standards of reporting. What about universal standards for terms and conditions or community rules? We could perhaps say, "If you post community rules, you have to stick to and live by your community rules". Is that a way to avoid the German problem, as we might put it, and get companies to do what they say they are going to do? Is that an interesting way forward?

***Mark Stephens*:** It is an interesting way forward and it is increasingly going to be an important way forward as we get to the internet of things, where our fridge or our home could be hacked. We may have a device that streams music or other communications into our homes. Increasingly, that kind of information is going to be available. Take cars, for example, and the data around them. It will be important that we have security around that data. Whether that falls into what some might call data protection laws, into encryption or indeed into consumer law, it probably has an overarching consumer perspective, because we should know what we are giving up and what the remedies are for breaches of those laws.

Q63 **Baroness Bonham-Carter of Yarnbury:** This is something that has come up in previous sessions. You have been talking about Google and Instagram, the big companies, but of course there are myriad little companies out there too. How do they feed into this? You sound quite optimistic about the way forward, although, Jenny, you mentioned that we have to be happy that we are being a bit reactive. I just wondered how the smaller companies fit into your scenario of self-regulation.

***Jenny Afia*:** I tend not to have a huge amount of dealings with the small companies, mainly because by the time a client comes to me they are concerned about information going out to a huge market. If it is a very small platform in terms of audience, they tend to have the fortitude to ignore it. I do not have a huge amount of experience of those small companies. I have experience of the pesky, annoying ones that are outside the court's jurisdiction and so on. The issue with small companies is to build in safety and privacy by design and hope the foundations are right for all companies.

Baroness Bonham-Carter of Yarnbury: I suppose this is going back to children and so on.

***Mark Stephens*:** Little companies are the vulnerable spot here. You are right to alight upon it. They invariably do not have the bandwidth or the resources to manage the challenges their technology may produce. This has been recognised in the ICT sector, where there has been a considerable amount of sharing of knowledge and technology, particularly when working in foreign markets, but also in relation to the terms of business. A small company may not have the capacity to pay many guineas to lawyers such as Jenny and me to draft terms of business, but they have the ability to share the technology of their terms of business and how they have developed. That goes back to the point that was made to me earlier about holding people to account to their terms of business. If they are state of the art, you can hold them to account to those contractual terms.

Q64 **Baroness Bertin:** I would like to start by declaring that I work for BT. Can we come back to the design point? We are all agreed that this could be a force for good but, let's face it, ethical design might not be the most profitable. It is about trying to work out who should be responsible for overseeing this process. What principles and values should define the safety by design principle?

***Jenny Afia*:** In terms of who should be responsible for overseeing the process, either we have a huge global regulator or it is on each sector. If we are talking about fridges, it might be the food standards industry; if we are talking about social media, it might be in the Digital Economy Act. In terms of the principles that should go into safety by design, from my perspective children's interests should be paramount, as recognised by article 24 of the European Charter of Fundamental Rights. It will not be any surprise that I, as a privacy lawyer, would like the right to privacy and to freedom of expression to be baked into privacy and safety by design.

***Mark Stephens*:** Increasingly, we are at a point where safety by design is coming forward. At the Global Network Initiative, we have encouraged companies to come forward with their proposals for the standards by which they should be judged. It is an evolving sector, as you will understand very clearly, but it is absolutely critical that we now start to have companies state exactly where they stand on these issues and what they are going to do to protect us. Whether that is, at one end of the scale, self-driving cars or, at the other end, the sorts of things Jenny is talking about, you have to have that design baked in, and increasingly it will be.

We then have the problem of how you communicate that. There is a whole issue around communicating what people are doing to protect you, but also what they are then going to do with your data. We have just seen the tip of a very large iceberg with GDPR. People have made a lot about it but, when you drill into those consents and see who is sharing the information and what they are doing with it, it is considerably broader than what anyone in the street really has any conception of.

Q65 **Lord Allen of Kensington:** In your opening statements, you both talked about the key principle of having the same protection online as offline. I am interested in understanding whether the current legislation affords that protection in both areas.

Mark Stephens**:** It does, by and large. That is where I came back—my analysis says this is the core principle. Can we identify a lacuna where that is not the case? We could take a topical example: upskirting. If you happen to be in England and Wales, and not in Scotland, it seems to me that, aside from it being a criminal offence, you might think digital dissemination of that should be a separate criminal offence. Therefore, that is something you might want to include in those kinds of things and it may be a gap in the law. I have not thought about it in enormous detail, but that seems to be something you could do. But there is no point in making extra laws just for the sake of extra laws. We have to say what we are likely to do.

To the point Jenny made right at the beginning, we do not know what will happen. We cannot predict the future; we are not prognosticators. We have to work with what we have and then encourage the companies, which to some extent share our own concerns about this, to ensure they are complying with their own terms of business.

Jenny Afia**:** We have the same theoretical protection online as we do offline, but the major issue is that the internet highlights the problem of the conflict of laws. If somebody in America defamed me in an after-dinner speech to a room of 30 people, I would have the same rights as if someone defamed me on an American blog. The principle is the same, but I would probably hear about it more if it happened on a blog. The internet brings into sharp focus the conflict between American laws and our laws, but theoretically we have the same protection.

Lord Allen of Kensington: Can I build on that? What are the practical challenges in prosecuting and suing people who have done something illegal or defamatory online? Can you explore that a little more?

Jenny Afia**:** It is incredibly difficult if they want to be anonymous. It is so easy to hide your identity on the internet, which makes taking meaningful action extremely difficult. You face the whack-a-mole problem and you are constantly chasing your tail. It means it is expensive, because you have to go after different platforms. There is also the effect we have dealt with for many years known as the Streisand effect: the fear that, if you take action to remove content on the internet, there will be a whole group of people who will delight in magnifying that content and making it a much bigger issue. There remain a lot of practical deterrents to even trying to have information removed.

Mark Stephens**:** We have seen a lot of this in relation to harassment cases. For example, a woman we were representing had defamatory comments made about her in the UK. They were injuncted. It kept going, so the police became involved. The individual fled to southern Ireland, where the police became involved again. He then fled to Hungary, where the matter has languished for the past several years with him firing shots at intermittent moments. I suppose the takeaway I have from that is that we need to look at the international co-operation between states both at a police level, with the European arrest warrant, and perhaps in relation to mutual legal assistance. After Brexit, although we will be a separate legislative nation, we need to maintain those connections to ensure our citizens do not lose out.

Q66 **Baroness Quin:** My question really follows on from the mention there of Brexit and the situation of the UK after that. What effect will the UK leaving the EU have on the regulation of the internet? I noted that Jenny mentioned the European Charter of Fundamental Rights, and mention has just been made of things such as the European arrest warrant and the difficulties of getting them to take effect sometimes. It is fair to say we have probably had two versions of life after Brexit. One suggests there will be problems because we will not have the same influence in rule-making as before and we will not have the strength of belonging to a big bloc; on the other hand, other witnesses have talked about us taking the opportunity to become a global leader in internet regulation. What are your thoughts about this?

Jenny Afia**:** I have personal views but not a huge amount to add from a professional perspective, other than that the Brussels recast regulation is in flux, and that will have huge implications for enforcing civil and commercial cases against defendants. I assume something will happen in relation to the Rome regulation. As to the UK's role in all of it, I will leave that for others more qualified than I am to opine on.

Baroness Quin: Can you elaborate on what you meant by the recast regulations, the timing of decisions that are likely to occur and whether they will occur at a time when we are in the EU or out of the EU?

Jenny Afia**:** I am sorry; I am confused.

Baroness Quin: What exactly were you referring to there? I did not quite understand it.

Jenny Afia**:** The Brussels recast regulation, I understand, is one of the pieces of law that allow us to take action against Facebook in Ireland. If that were to change post-Brexit, it would be harder to take action.

Baroness Quin: I see. Is that something you have also thought about?

Mark Stephens**:** Yes; all the major American technology companies are based in Ireland, principally for tax reasons. As a consequence, if you wish to enforce, you invariably have to go to Dublin to do so, because that is effectively the chosen epicentre of the west coast companies. Being out of the EU, or it becoming more challenging to take those enforcement proceedings in a non-European Union context, could make things very difficult.

There are a couple of things I would add in order to address your question. The Americans are moving inexorably towards EU standards. They have recognised that they have to broadly comply with the GDPR if they are international businesses. If they are domestic American businesses, that is very different. The e-commerce directive, the e-privacy directive and other EU legislative standards are coalescing around an international norm. As one of my friends, a New York judge, said to me, "When in Rome, do what the Romanians do". That is where the American internet companies are getting to, and they will align themselves with European legislation because they do not want to go as far as some of the other countries that are popping up, whether that be Russia, China, Turkey or wherever. They see that as a good middle ground.

For us, it is about ensuring that our citizens have the protections they have now afterwards. I do not see the EU allowing us or us wanting us to become some kind of state where we are allowing a wild west of the internet or, the other way, going to a more regulated environment. If we go to a more heavily regulated environment than the rest of Europe, in those circumstances, we will drive the economies yet further offshore because they will migrate to those more beneficial, benign regulatory environments.

Baroness Quin: Whether we are in or out of the EU, we are likely to remain fairly close in terms of regulations and legislation.

Mark Stephens**:** That is right. In order to do business with the EU, we will clearly have to comply with its GDPR and other e-commerce-type standards. This is one of those spaces where, while we may have our sovereignty and be able to make a decision, the wise decision is to maintain the standards of equivalence that the EU has.

Q67 **Lord Goodlad:** This is perhaps a question for Jenny, who has given us evidence on the jurisdictional challenges of applying British law to social media companies and other intermediaries. Most of them seem to opt for the United States courts as where the proper law of the contract, or whatever it is, should be. How do you see the way through this, if at all? Secondly, what should be the function of international organisations in the regulation of the internet, and the role of the British Government? Should it be the OECD or somebody else?

Jenny Afia**:** I am struggling to see a clear way through the challenges of applying English law. Unless we are willing to have huge, substantive change, I do not see how we get over an issue such as the SPEECH Act, for example, which was introduced several years ago. It put trying to enforce a defamation judgment on a par with an act of terrorism, if you try to enforce your rights in America. That was introduced by President Obama. It is a huge issue that we have faced for many years. The way we have dealt with it on the ground is we have had to ignore what is going on in the rest of the world.

A couple of years ago there was the case of PJS v News Group Newspapers, which went to the Supreme Court, which was all about trying to protect private information. The media argued very strongly that it was farcical to try to do so when the rest of the world, and even people in England going on Twitter, could view the content you were trying to stop. The court reached what in my view was the correct decision: that is as may be, but currently we are in a position to exert control over the British media and we think there is still a virtue in doing that. We are sort of dealing with the problem by just trying to control what we can and resigning ourselves to the rest of it. It is not a satisfactory solution, but I am afraid I do not see a way out of it.

Lord Goodlad: Do you see any role for the OECD in all this?

Jenny Afia**:** I do not see a clear one.

Q68 **Lord Gordon of Strathblane:** Can I ask a supplementary? As a non-lawyer, if I take copyright, where the thing originates is irrelevant. It is where it is heard that you incur the copyright charge. Surely the same should be true of offensive material on the internet. Would the same logic not apply?

Jenny Afia**:** You would think so, but material that is subject to copyright is very easy to have removed from the internet because America places great value on intellectual property. Often, the way we try to get around the problems with protecting privacy is to find a way to assert copyright. It should be the same approach. It seems odd that it is not.

Mark Stephens**:** It is important to recognise that the SPEECH Act only applies to defamation; it does not apply to privacy. If you get a privacy injunction here in London, it will be enforced, along with the damage award, in America. The challenge we are likely to encounter is in relation to long reach and the jurisdiction. At the moment, with the PJS case that Jenny adverted to, we are limited to an injunction in the United Kingdom. But I found myself at Hudson News at JFK when that magazine came out, and there was a jumbo jet queue out of the door of people buying the magazine and bringing it back to London. That is problematic, and that is a real-world example of what is happening on the internet.

I know we are here talking about British law and how we change British law, but there is another issue here that we have to think about. If we start to take Turkish, Egyptian, Iranian, Russian or Chinese law and their decisions, and incorporate them and respect them here, there is going to be a challenge. Throwing away the jurisdictional reach of our laws needs very careful consideration before we do it.

Q69 **Baroness Kidron:** At the beginning, both of you said that there is not really a call for new regulation. Forgive me for doing a bit of a "best of", but you talked about harmonising laws, lacunae, universal standards, the IoT consumer piece and enforcement. We can go through a whole shopping list of things you have both suggested might require doing. I want to finish by coming back to the question of who is responsible. Who holds this brief? One of the things we keep on hearing is that it is so split across people: some of it does not sit with anyone, and then it sits with lots of different people.

Finally, to Jenny's point about reactivity versus proactivity, is there an argument, as we have heard from some witnesses and definitely in some written evidence, for having a new person, whatever the outcome is on regulation, to hold the brief for all this in one place and to work their way carefully through all these issues? You are asking for a certain level of proactive action, reaction and thoughtfulness around the whole piece.

Jenny Afia**:** The brief would be for that person to be an anticipatory body. There is a real need for horizon scanning and to look ahead, so we are not just dealing with these issues through piecemeal legislation and the 11-plus bodies that touch on the internet. If that is the brief, it would be fantastic to have a body that was charged with looking forward and anticipating issues. That body would work with the existing regulators to ensure they had sufficient digital skills and could harmonise and provide an overview. That would be fantastic. It almost feels like a luxury, when you start seeing how much work is already going on. When we are talking about such important issues, maybe it is essential.

The Chairman: Horizon scanning is clearly important in this area, whether it is an individual or a body horizon scanning. Would they be well guided by a set of principles—either drawn from existing principles or a new set of societally agreed principles—that they are trying to apply to how they see the future developing in so many of these areas?

Jenny Afia: Yes, but I would say those principles are probably human rights: the right to privacy, the right to respect for private and family life and the right to dignity. They are the rights we already have. We do not need new principles.

The Chairman: It is all already there.

Mark Stephens: You are right: there is a "pulling the strings together" piece that needs to be done here. In your first question, you asked about regulation. The question here is how you draw those things together, such that it ends up being a more fleet-of-foot and proportionate response to the huge number of challenges, some of which we have isolated today.

I hate to suggest it, but we could have an internet tsar with an obligation and a remit to do some scanning of the horizon, and to look at whether the terms and conditions of business that ordinary folk do not read—I was going to say "none of us", but we do—and just click "accept" are acceptable and being complied with. This internet tsar could build those relationships with the internet companies to draw attention to and understand where problems are, and alert Parliament where there are lacunae coming up or where there are problems, so you have an independent voice saying, "Actually, we need to do something about this" or "Actually, we can deal with this in another way". That is perhaps the most effective way of achieving a positive outcome to what is obviously a shared concern. At the end of the day, everybody wants the right outcome; everybody wants to remove material that is unacceptable.

The Chairman: Thank you. We are drawing to a close, because our next witnesses are here.

Q70 **Baroness McIntosh of Hudnall:** This is very brief. Maybe there is no answer or you could write to us with an answer, but I was just wondering about case law. What quantum of case law exists already, in respect of any of the issues we have been discussing? Who, if anybody, knows what that quantum is? How is it held and how is it accessed?

Jenny Afia: There is quite a body. I would be very happy to write and provide details.

Mark Stephens: One of the challenges is that the law is developing down different routes in different countries. We need a greater overview to inform the Committee, and more broadly, about the different ways the same problems are being dealt with in the same places.

Baroness McIntosh of Hudnall: Anything you can tell us about it would be welcome.

The Chairman: On behalf of the Committee, can I thank both of our witnesses for very helpful and very concise evidence, which we will certainly be relying on as we take the inquiry forward? We would welcome any further points that you wish to make. Please feel free to write to us if there is anything you think we omitted in our questioning, or anything in hindsight that you might have included in your answers. We have a voracious appetite for reading so, similarly, if there is any material published in your domain that you think might be of interest to the Committee, it would be helpful if you sent it to the clerk.

We have learned that there is somebody out there who reads the terms and conditions. Up until now, we were told that nobody reads them, so that was useful too. Thank you both very much indeed. Your evidence was very helpful.

IAB UK – written evidence (IRN0097)

Background

1. IAB UK is the trade association for digital advertising, representing over 1,200 of the UK's leading brands, media owners, technology providers and agencies. Our purpose is to build a sustainable future for digital advertising, a market that was worth £11.55bn in the UK in 2017.

2. The IAB is actively engaged in working towards the optimal policy and regulatory environment for the digital advertising market to continue to thrive. We also seek to promote good practice to ensure a responsible medium.

3. Our submission focuses on two main aspects of the terms of reference as they relate to digital advertising: legal liability, and the use of personal data.

Regulation of digital advertising

4. As the Committee's call for evidence recognises, existing regulation and self-regulation applies online. There are a number of key pieces of legislation that apply to digital advertising, including in relation to data and privacy, consumer protection, and 'information society services'. As the call for evidence notes, digital advertising is also regulated by the Advertising Standards Authority (ASA) which enforces the UK Code UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing (CAP Code). The CAP Code reflects the provisions of the Consumer Protection from Unfair Trading Regulations 2008 which prohibit certain unfair and misleading practices, and requires that all advertising – including online – is obviously identifiable as such. There is also self-regulation in the digital advertising sector in relation to providing people with transparency and control over online behavioural advertising (see Appendix 1).

5. The industry continues to develop its self-regulatory initiatives to respond to challenges. For example, in March this year, a new joint initiative was announced between JICWEBS[832] and the U.S.-based Trustworthy Accountability Group (TAG). In the area of ad fraud, TAG has set up the Certified Against Fraud Program, involving anti-fraud guidelines, and a trust seal which means companies can publicly communicate their commitment to combatting fraudulent non-human traffic in the digital advertising supply chain. JICWEBS and TAG have committed to working together to on transfer learnings between the respective initiatives to improve their effectiveness and create a united and consistent approach across markets to tackle criminal activity and clean up the digital ad supply chain.

6. **We believe that the existing regulatory framework for digital advertising is robust, proportionate and effective. This is complemented by industry-led self-regulation, which has expanded over time in response to new issues and enjoys wide support within the ecosystem. We believe this approach is appropriate to ensure that the digital advertising industry operates responsibly and can have a sustainable future.**

[832] The joint industry committee that oversees self-regulatory initiatives including developing good practice principles and certification in relation to brand safety, ad fraud and viewability. See https://jicwebs.org/.

Digital Charter

7. We share the Government’s ambition to make the UK the best and safest place for online advertising and the digital advertising sector has worked with others in the advertising industry, under the auspices of the Advertising Association, to identify areas where the Government could support industry efforts to tackle some of the issues that threaten to undermine consumer and business trust in digital advertising.[833] These can be summarised as:

- Ad fraud: ensure appropriate law enforcement action is taken against criminals who abuse the digital advertising ecosystem for financial gain

- Ad misplacement: support existing initiatives and encourage compliance with industry standards and good practice (e.g. the JICWEBS DTSG Brand Safety Good Practice Principles)

- Ad blocking: maintain equivalence with the EU ‘net neutrality’[834] rules post-Brexit; recognise the value of the ad-funded business model, which supports the development and provision of digital services, content, and apps; support publisher efforts and wider industry work to improve the ad-funded experience online through the Coalition for Better Ads

- Data privacy: prioritise discussions on data-sharing in Brexit negotiations and allocate resource to ePrivacy Regulation negotiations (see paragraph 28 below).

Legal liability of online platforms

8. Digital advertising operates within a complex ecosystem and relies upon the collaboration of multiple players including advertisers, ad buyers, demand aggregators, supply aggregators, technology providers, creative agencies, measurement and assurance providers, and media owners.

9. A range of legal and self-regulatory frameworks, as well as technical standards, serve to support this ecosystem. Among the foundational legal frameworks is the regime which governs the assignment of rights and responsibilities within the digital ecosystem. This is enshrined in Articles 12-15 of the eCommerce Directive, and is expressed as limitations to liability for online intermediaries, but in practice balances rights and responsibilities between a far broader range of players in complex digital environments. It is important that the Committee appreciates the broader application of this legal framework and its particular relevance to digital advertising.

10. This legal framework has characteristics which make it adaptable to a range of digital environments, including advertising. By engaging specific activities, rather than a particular business model or technology platform, it is technology neutral and applies

[833] See https://www.adassoc.org.uk/wp-content/uploads/2017/12/AA_Digital_Charter_2017_SinglePages_15.11.17.pdf

[834] Net neutrality is an important principle that protects against network-level ad blocking (e.g. at mobile network operator level) and existing guidelines, based on the EU ‘Universal Service Directive’, state that all internet users should have equal access to content and advertising online to ensure telecoms operators cannot block content.

in a targeted way. This means that companies with complex business models – where they may be an intermediary for some activities but not for others – can confidently apply the principles to different activities they perform and have legal clarity. For example, a company that has a news publishing business and also has an ad platform business would be legally responsible (in this specific example) as a publisher for its editorial content but could also be an intermediary (with differentiated liabilities) for certain activities relating to the operation of its ad platform.

11. Crucially, the principles of this framework are woven into a range of industry initiatives and self-regulation including the UK CAP Code on non-broadcast advertising. The Code assigns primary responsibility for advertising content and decisions about targeting to the advertiser, whilst engaging media owners, for example, to help enforce ASA adjudications and terminate non-compliant campaigns where an advertiser fails to act, or engaging advertising intermediaries to surface evidence to aid investigations into breaches of the Code. Similarly, the EDAA principles on behavioural advertising (see Appendix 1) commit advertisers to defined obligations around targeting decisions whilst also place other obligations on advertising intermediaries that reflect their role and position in the ecosystem.

12. In the context of editorial control, tensions can arise between the liability principles that apply to 'information society services' (e.g. under Article 14 of the e-Commerce Directive) and questions around how illegal content online should be managed or moderated. Actions taken in good faith by service providers could potentially be aided by having an equivalent defence to that in Section 230 of the U.S. 1996 Communications Decency Act that affords a 'Good Samaritan' protection for blocking and screening of offensive material. The Committee could explore the feasibility and benefits and drawbacks of this approach.

13. The principles of the underlying legal framework set out in the e-Commerce Directive provide the foundations on which self-regulatory initiatives are built and give confidence to the parties involved to collaborate to resolve challenges which arise in digital advertising. These are not legal issues which could easily be addressed contractually in such a complex commercial and technical environment. Shifting away from the activity-based approach, or modifying this regime for some types of technologies and/or business models but not others, would have a disruptive and unpredictable impact on the digital ecosystem and the ability of its component operators to collaborate. **The IAB would urge the Committee to proceed with a high degree of caution on this issue.**

Regulation of the use of personal data in digital advertising

14. The use of data and the protection of privacy in digital advertising is currently governed by the Data Protection Act 1998 (shortly to be superseded by the General Data Protection Regulation (GDPR)), and the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2003 (PECR) (which derive from European Directive 2002/58/EC, also known as the 'ePrivacy Directive'). Both are enforced by the Information Commissioner's Office in the UK.

Data protection law

15. The Data Protection Act 1998 governs the collection and processing of data and will shortly be superseded by the General Data Protection Regulation (GDPR), which comes into force from 25 May 2018 in all EU member states, including the UK.

16. The GDPR updates the existing EU data protection framework and aims to give individuals more transparency about and control over whether and how their personal information is used. It regulates the use of all personal data in digital advertising (information such as an online identifier – e.g. an IP address – can be 'personal data'). Some of the key provisions introduced by the GDPR, and that are relevant to digital advertising, are:

- Organisations will require a legal basis to process personal data. There are six legal bases available, but those most commonly used in the digital advertising sector are 'consent' and 'legitimate interests'.

- The GDPR strengthens the conditions for consent. Consent will need to meet very high standards (e.g. it cannot be bundled with Ts&Cs) to be relied on as a legal basis for processing personal data. The user will also need to give consent 'unambiguously' with an affirmative action. Processing 'sensitive' personal data (e.g. racial or ethnic origin / sexual orientation) requires the user's explicit consent.

- In all cases, evidence that consent has been obtained will have to be recorded, meaning organisations that have no direct relationship with the user will have to find a way to obtain consent indirectly.

- The introduction of increased sanctions: organisations can be fined up to €20m or 4% of annual turnover (whichever is greater) if they breach the law.

- The GDPR also introduces special protection for children's personal information: if an organisation collects information about a child and is relying on consent to process it lawfully then it will need a parent's/guardian's explicit consent where the child is under a specified age (expected to be 13, in the UK).

17. The GDPR applies to both 'data controllers' (i.e. an organisation that decides how and why personal data is processed) and – for the first time – 'data processors' (i.e. an organisation that specifically acts on a controller's behalf). Businesses involved in the processing of personal data for digital advertising purposes will be classified as either a data controller or a data processor under the GDPR.

18. Obligations for data controllers include transparency – the GDPR extends the amount of information organisations must provide to individuals about how they use personal data (e.g. an organisation's legal basis for processing personal data, data retention periods, the use of third party data etc.) – and accountability. The GDPR also requires that information given to people about the processing of their personal data is easy to understand and written in plain language.

19. IAB UK has produced a briefing[835] on GDPR and digital advertising, which is enclosed with this submission. We draw the Committee's attention in particular to the

[835] https://www.iabuk.com/policy/eu-general-data-protection-regulation-gdpr-briefing-digital-advertising-industry

following sections, which provide more detail about what the GDPR means for digital advertising, the additional responsibilities it creates for data controllers and processors, and the extensive rights that it confers on individuals.

- Section 4 – Legal Bases
- Section 5 – Obligations for Data Controllers and Data Processors
- Section 7 – Individual Rights & Control

20. In addition, the IAB's GDPR preparation checklist[836] explains in detail the key aspects of the GDPR as they relate to businesses in the digital advertising sector.

21. **The provisions in the GDPR mean that individuals will have more information about and control over whether and how their data is used.**

Cookies and other similar technologies

22. PECR sets out specific rules on rules on the storing of information or gaining access to information already stored on a device (whether personal data or not), i.e. cookies and similar technologies (in this submission we use 'cookies' to mean either or both of these). Cookies are widely used in digital advertising, for example to help personalise advertising and measure its outcome.

23. PECR requires that users are told if a site, app, etc. wishes to drop a cookie or access a stored cookie on their device, and given a clear explanation of what the cookies do and why (this is usually managed via a 'cookie banner' that you see when you visit a website). Specifically, the site must get the user's consent to store or access a cookie on their device.837 The GDPR does not supersede PECR and it remains in force in the UK as well as other EU countries that have implemented it. However, the GDPR changes the definition of 'consent' as it applies to PECR and the use and access of cookies.

24. In practice, this means that – from 25 May 2018 – consent has to be sought from the individual before a cookie is set or accessed. That consent, under GDPR, has to be freely given, specific, informed and unambiguous and requires a positive action from the individual to be valid.

25. **Taken together, the provisions of the GDPR and PECR mean that individuals will know when and how their personal data is being or could be used for digital advertising purposes, whether by a first party (e.g. the site or platform that they are accessing) or a third party (e.g. an advertising technology company) and will have the ability to choose whether and how their data is used (and to change this at any time).**

The effect of Brexit

26. The regulation of the use of personal data is, as outlined in our submission, key to the regulation of digital advertising.

[836] https://www.iabuk.com/policy/iab-uk-gdpr-checklist

[837] There is an exception for cookies that are essential to provide an online service at someone's request (e.g. to remember what's in their online basket, or to ensure security in online banking).

27. The digital advertising ecosystem is a global business and relies on the free flow of data. The free flow of data between the EU and the UK (in both directions) will be crucial. We welcome the inclusion of data flows as one of the top five Brexit issues and the commitment to implementing the GDPR in full and maintaining regulatory alignment.

28. We welcome the Committee's recommendations in its previous report. 'UK advertising in a digital age', that the UK Information Commissioner's Office should retain a place on the European Data Protection Board following the UK's exit from the EU.

29. We also share the Committee's concern, as set out in that report, that Brexit will cause the UK to lose its influence in setting EU rules for data protection which the UK is likely to remain aligned with post-Brexit. This is particularly relevant in relation to the proposed ePrivacy Regulation (ePR), which will review and update the ePrivacy Directive (the basis for PECR) and would apply across all EU member states. The proposed ePrivacy Regulation threatens the future of the data-driven digital economy and could greatly undermine the investments made in GDPR implementation efforts. Even though the UK may have left the EU at the time of its application, UK businesses may in practice have to adhere to it to ensure continued provision of services to EU markets. As such the development of the Regulation still needs the full involvement of UK authorities. **This is critically important as the Regulation passes through crucial stages of the negotiations**.[838]

30. In practice, many digital advertising companies operate across EU markets and globally, and a consistent and harmonised regulatory approach is preferable, particularly in terms of issues such as data and privacy. However, these approaches also need to be pragmatic and take a proportionate approach to managing relative risk. **Brexit may present an opportunity to improve on existing or potential new laws, such as the ePrivacy Regulation, and this should be balanced against the risk of developing fragmented or disparate legal frameworks, particularly in the context of the internet, which is by its nature global and without borders.**

[838] https://www.iabuk.net/news/european-parliament-committee-s-approach-on-eprivacy-would-harm-european-media-and-citizens

Appendix 1: EDAA Framework for Online Behavioural Advertising

In addition to legislative requirements and the mandatory self-regulatory system of CAP and the ASA, the digital advertising industry has established self-regulatory frameworks in other specific areas in order to set out accepted standards and good practice for responsible advertising. One such framework covers the use of personal data for online behavioural advertising.

IAB UK acknowledges that the collection and use of consumer data (such as web browsing and other information) could potentially raise issues relating to consumer privacy. In 2011, building on an US initiative and the development of good practice in the UK, EU advertising and media trade bodies published good practice for all EU and EEA markets to enhance transparency and user control for online behavioural advertising (OBA). This framework applies to advertising targeted at any user, including those aged under 18, with specific provision relating to younger children, as described below.

The initiative is based upon seven key principles:

i. Notice: Transparency about data collection and use practices associated with behavioural advertising, providing consumers with clear, prominent and contextual notice through multiple mechanisms, including an icon in or around advertisements linked to further information and control mechanisms.

ii. User choice: Greater consumer control over behavioural advertising. For example, via www.youronlinechoices.eu.

iii. Data security: Appropriate data security and retention of data collected and used for behavioural advertising purposes.

iv. Sensitive segmentation: This principle recognises the need for additional protection for younger children, and requires participating businesses to agree not to create 'interest segments' to specifically target children (12 and under) and on the collection and use of sensitive personal data for behavioural advertising.

v. Education: For consumers and businesses about behavioural advertising and the self-regulatory Framework.

vi. Compliance and enforcement: Mechanisms to ensure the effectiveness of the Framework, including a trading seal to be granted to compliant businesses once independently audited and which demonstrates to other businesses that the holder adheres to the obligations under the Framework.

vii. Review: Regular review of the Framework to ensure it evolves with developing technology and business practices. For example, in 2016 the EDAA extended the existing principles to the mobile environment, so that they apply to ads shown on smartphones and tablets in addition to desktops and laptops.

A copy of the EU industry Framework can be found at: http://edaa.eu/european-principles/. At the heart of this work is a symbol or icon (see below right – often known as the 'AdChoices' icon) that appears in or around the advertisements on sites, as well as on site pages themselves. When a user clicks on the icon he or she will be able to find out more about the information collected and used for this purpose. In 2017, over 170bn icons were delivered by approved providers across Europe, giving consumers significant opportunities to manage or control their online advertising preferences.[839]

5.6 The icon also links to ways for internet users to manage their interests, such as via privacy dashboards or ad preference managers. It also links to a pan-European website – www.youronlinechoices.eu – with helpful advice, tips to help protect privacy and a control page where you can turn off behavioural advertising. There are on average 1.9 million unique visitors to www.youronlinechoices.eu every month.[840] The UK version of the website is at www.youronlinechoices.eu/uk. Further information on the initiative is available at https://www.iabuk.com/policy/iab-factsheet-may-2014-online-behavioural-advertising.

The EU industry initiative is administered by the European Interactive Digital Advertising Alliance (EDAA) www.edaa.eu. The ASA administers OBA consumer complaints in the UK and in 2013 new rules on OBA were introduced to the CAP Code to ensure businesses provide:

- notice to be provided to web users **in or around the advertisement**;
- choice via an **opt out mechanism** to prevent data from being collected and used for behavioural ad purposes.

These rules are **complementary** to the EU Framework: those businesses complying with the EU Framework will be complying with the CAP Code.

It should be noted that it remains to be seen whether and how this Framework will operate once GDPR comes into effect, as a number of the aspects that it covers (such as notice, choice, and sensitive segmentation) are now covered by the GDPR. [841]

May 2018

[839] https://www.edaa.eu/ext/edaa_2017.html

[840] ibid.

[841] In response to changes introduced by the GDPR, the Committee of Advertising Practice (CAP) is consulting on changes to the rules related to the collection and use of data for marketing. https://www.asa.org.uk/news/gdpr-consultation-on-the-collection-and-use-of-data-for-marketing.html

Information Commissioner's Office (ICO) – written evidence (IRN0087)

About the ICO

The ICO's mission is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The ICO is the UK's independent public authority set up to uphold information rights. The Information Commissioner does this by promoting good practice, ruling on complaints providing information to individuals and organisations and taking appropriate action where the law is broken.

The ICO enforces and oversees the Freedom of Information Act, the Environmental Information Regulations, the Data Protection Act and the Privacy and Electronic Communication Regulations.

Introduction

Thank you for the opportunity to take part in this important consultation.
We agree that a discussion of internet regulation is an important and relevant one. In our response we aim to provide you with an insight into the ICO's role; what can and is already being done to protect individuals' online privacy.

In answering your specific questions we have primarily focused on matters that fall within our area of statutory responsibility, primarily as regulator for data protection law in the UK.

Specific questions

Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

The ICO is the UK's regulator for data protection and as such has a key role in the regulation of the internet, when it relates to the processing of personal data online.

The Data Protection Act 1998 (DPA), soon to be replaced by the General Data Protection Regulation (GDPR) and the Data Protection Bill currently making its way through Parliament, all provide the Commissioner with a broad remit and powers to help protect personal data online. There is regulation of the internet in respect of data protection - GDPR strengthens the obligations and accountability of data controllers, enhances the rights of individuals and strengthens the powers of the Commissioner.

Because of the above, any proposed further regulation of the internet, would need to ensure it complements and not duplicates the functions that the Commissioner has.

The question of the desirability of regulating the internet is a complex one. One of the main aims of the internet at conception was the free, uninhibited exchange of information. There are important questions about the balance between further statutory regulation and what role self-regulation should have, involving softer measures such as codes practice. The Commissioner believes that both have a role to play, combined with other measures such as improved digital literacy.

There is growing consumer unease about how online platforms are using personal data and potentially limiting consumer choice. Research conducted by the Commissioner shows less than one in ten (8%)[842] of UK adults say they have a good understanding of how their personal data is made available to third parties and the public. Improving transparency is a key aim of the forthcoming GDPR.

The risks thrown up by the current internet ecosystem also go beyond compliance with data protection law and trigger wider ethical considerations and how this drives trust.

The activities of online platforms are therefore not entirely unregulated, but it is fair to say that some aspects of the law have not kept pace with the rapid development of the internet. In terms of data protection GDPR is an important step forward to catch up.

Search engines are no longer simply that and social media organisations can no longer be described as purely host platforms. They filter news, micro-target advertising, and in most cases facilitate and generate content.

Where these activities use personal data it is important to be clear that data protection law applies and can provide effective protection for individuals. Recent case law, such as CJEU case of Google Spain, has made clear that online platforms such as search engines are data controllers under data protection law. They can be fully liable for their use of personal data. This has enabled individuals to exercise their rights, including a 'right to be forgotten' to request that personal data is removed from platforms. These rights are strengthened under the GDPR.

The Commissioner recognises that there is a role for regulation of internet content, beyond data protection, and the wider information fiduciary duties of the online platforms must be considered.

The global nature of the internet may raise territorial difficulties in terms of jurisdiction and the ability to enforce regulation. The GDPR will operate under the concept of the 'one stop shop' – creating a 'lead data protection authority' for organisations established in the EU and providing services across EU borders.

Where organisations are not established in the EU, territorial scope under the GDPR is still broad – any organisation directly providing online services to individuals in the EU will be covered. The challenge for the EU is to establish the enforcement mechanisms to make this work in practice outside the EU, which may require multi-lateral agreements.

What should the legal liability of online platforms be for the content that they host?

Online platforms are no longer just platforms allowing individuals to access content. As mentioned above they also produce content, filter what individuals view and in some

[842] http://www.comresglobal.com/polls/information-commissioners-office-trust-and-confidence-in-data/

cases micro-target individuals with advertising. The Commissioner considers that, beyond compliance with data protection law, these organisations have a legal and an ethical duty to treat people's personal data appropriately.

These organisations have control over what happens with an individual's personal data and how it is used to filter content - they control what individuals see, the order in which they see it and the algorithms that are used to determine this. Online platforms can no longer say that they are merely a platform for content, they need to take responsibility for the provenance of the information that is provided to users. Looking beyond data protection, the Commissioner would propose exploring a range of solutions to make organisations more accountable for the content they produce, involving soft and hard measures, to enable the balance between responsibility and freedom of expression to be fully addressed. The ICO recognises that platforms are already taking responsibility for content, beyond data protection law, such as removing extreme content and hate speech but more evidence is needed to understand how these new measures are working in practice.

How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

The Commissioner has also published guidelines for search engines, explaining how to consider requests for links related to individuals to be removed from search results, which provides an example of how to balance competing rights in the context of internet regulation.[843]

There is a particular requirement under GDPR for online content to be appropriate to its audience, particularly where that audience is part of a vulnerable group, for example, children. Both the GDPR and the Data Protection Bill have specific requirements in relation to children. Article 8 GDPR provides additional protections in respect of the provision of information society services to children, including parental consent. Recital 38 GDPR makes clear that children merit further protection in relation to their personal data, in particular its use for '…the purposes of marketing or creating personality or user profiles…'. As the Data Protection Bill currently stands it also requires the Commissioner to produce a code of practice about age appropriate design relevant to online services. This responsibility will be unique in the EU, and important in setting standards for websites and services targeted at children. The UK has an opportunity to be a leader in this context.

What role should users play in establishing and maintaining online community standards for content and behaviour?

The Commissioner is supportive of involving users in this process. The internet enables people to interact with each other and creates unprecedented numbers of relationships, often without meeting the people they connect with. Many disputes that emerge about

[843] https://ico.org.uk/for-organisations/search-result-delisting-criteria/

online content can relate to information that individuals post about each other. Education and standards therefore play an important role beyond the law.

The process of undertaking data protection by design and data protection impact assessments, required under GDPR, should also place the user at the heart of any process involving use of personal data.

What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

As discussed above, the Commissioner sees what online platforms do about online content and the use of personal data as a freedom of expression issue as well as a data protection one. It is important that online platforms ensure that individuals can clearly understand and control any profiling or filtering that can affect the types of information they see as part of personalised content. It is important in a democratic society that people are not left uninformed of varying views and opinions, to avoid echo chambers that can fuel divisions.

In conjunction with this, the concept of open data and open information is an important one. Being available to view and use information in a free and open manner is beneficial for society, democracy and business. An internet that is open and transparent ensures that people have a greater understanding of the key issues and challenges that different parts of society face and can lead to more informed debate between different groups.

What information should online platforms provide to users about the use of their personal data?

The GDPR has a clear focus on requiring organisations to be upfront and transparent about their use of individuals' personal data and to give individuals greater control over their personal data.

In particular, the GDPR includes the right to be informed (this is mainly covered by articles 13 and 14 of GDPR). The Commissioner has produced guidance[844] which discusses this in more detail. Essentially, the GDPR requires organisations to be clear about what they do with individuals' personal data, how they do it, on what basis they do it, what data they hold, how long they will hold it for and who they will share it with (this is not exhaustive). Beyond this, organisations are required to give any further information that is needed in order to make the processing of personal data fair.

Organisations should be giving individuals this information as soon as possible. A specific means of providing this information is in a privacy notice, which outlines all of the requirements of articles 13 and 14 in a clear and concise manner that is written in plain language and aimed at its intended audience. The Commissioner has produced detailed guidance[845] on the right to be informed, which provides advice and guidance

[844] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

[845] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/

on the best way of providing this information. The code also encourages organisations to be innovative in providing this information – embedding and layering the information as part of the design process, not just in one long notice.

The Commissioner considers that organisations should be as open and transparent as possible and view the opportunity to be transparent as not only achieving compliance in a data protection sense but also as an opportunity to engender trust and improve relationships with their customers.

In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

The Commissioner is currently undertaking an investigation into political campaigning and the use of personal data and data analytics online[846]. As this is an ongoing investigation the Commissioner cannot comment in detail, however, it is already clear that significant concerns exist about the transparency of micro targeting and political content. Our report will be published in June 2018. Enforcement actions taken against individuals or organisations will follow the publication of the report.

Online platforms must be transparent in the way they are using both their customers' data and other sources of personal data they combine it with. For example, under the 'partner category' system for Facebook advertising user data was combined with data from credit reference agencies to inform ad targeting. In the Commissioner's political targeting investigation, the Commissioner raised concerns about the lack of transparency in this program; in March 2018, Facebook announced it was discontinuing the partner category program.

The GDPR focuses heavily on the importance of transparency and accountability and increases the rights individuals have over how their data is to be used. The GDPR gives people the right to object to organisations using their personal data, the right be forgotten (the right to erasure of personal data) and the ability to challenge decisions made by machines and algorithms. It also requires the use of tools such as data protection impact assessments and data protection by design and default to address risks to privacy.

The issue of the use of algorithms and more generally, automated processing of personal data, is a key area where organisations must be clear with individuals about their use and the purpose of their use. Article 22 GDPR provides rules around the processing of personal data by automated decision making (including profiling of individuals). It requires that solely automated decisions should not be made, where it produces legal effects or similarly significant effects. Furthermore, such personal data processing can only take place where it is in relation to the performance of a contract, is allowed by EU or member state law or is based on explicit consent.

Beyond this, the right to be informed includes the right to be told of such processing and to receive meaningful information about the logic involved in the decision making as well as the significance and envisaged consequences of such processing.

[846] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/05/ico-statement-investigation-into-data-analytics-for-political-purposes/

Organisations who process personal data by means of algorithms without human intervention must be aware of this requirement and comply with it.

The Commissioner is working with the Turing Institute on guidance about the explainability of algorithms, to be published later this year. This is a challenging topic – technical information will not engage the average user. Transparency measures must explain data inputs, how outputs will be used and what the implications are. Innovation will be needed to do this clearly and engage users. Informing the users at a non-technical level must be paired with a deeper requirement to explain and account to the regulator. Under the new Data Protection Bill the Commissioner will have stronger powers to undertake inspections of online systems to examine how algorithms work in practice and act on behalf of the user.

The Commissioner provided detailed submissions[847] to the House of Commons Science and Technology Committee inquiry into algorithms in decision-making in April 2017.

However, as well as transparency and strongly linked to it, the Commissioner would encourage organisations to give individuals greater control over what happens to their personal data, without the need to formally exercise their rights. Control can be provided in the form of dashboards and other online tools within mobile applications.

What is the impact of the dominance of a small number of online platforms in certain online markets?

The Commissioner is concerned about the pervasiveness of big data analytics and micro targeting and the impact on the democratic process in particular. A small number of online platforms increasingly play an important role in how the public receive news and information, plus engage with online content during elections and campaigns. The platforms therefore have a key responsibility to ensure an effective balance between freedom of expression and other competing rights, including data protection.

A small number of online platforms dominate the market and have broad and deep collections of personal data that they can use to profile and target individuals. These concerns are magnified by mergers and acquisitions where personal data is the primary asset. The Commissioner recently took action over proposed data sharing between WhatsApp and Facebook, following WhatsApp's acquisition by Facebook. The Commissioner found the proposed data sharing between the two companies failed to comply with transparency and consent rules under the Data Protection Act. As a result of the Commissioner's investigation, WhatsApp signed an undertaking not to share personal data until these issues are addressed[848].

What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

[847] https://ico.org.uk/media/about-the-ico/consultation-responses/2017/2013970/ico-response-house-of-commons-science-tech-algorithms-20170410.pdf

[848] https://iconewsblog.org.uk/2018/03/14/whatsapp-signs-public-commitment/

The Commissioner has set out her views to Parliament in a number of submissions previously[849] – she most recently gave evidence to the Exiting the EU Select Committee on 9 May[850].

Leaving the EU could have a significant impact on regulation of the internet. Firstly, when the UK leaves the EU and becomes a third country it will no longer benefit from the legal certainty that EU member states enjoy under data protection law. This allows data to flow freely between member states and no legal assessment is required before data is transferred. As a third country the UK will need to demonstrate how its data protection regime is essentially equivalent to EU law, to enable it to gain a statement of 'EU adequacy'. This would then allow personal data to continue to flow without restriction. Without an adequacy decision organisations in the UK who want to receive personal data from the EU would need to rely on more burdensome measures such as standard contractual clauses and binding corporate rules.

Whilst this would enable data flows between the EU and the UK the Commissioner supports the Government's ambition for a bespoke agreement with the EU on data protection – this would include adequacy and also enable the Commissioner to participate in the one stop shop system within the EU. Participating in this mechanism would allow UK businesses operating online to work with a single regulator and the public could complain to the Commissioner about online services provided by EU based companies.

The Commissioner would also lose significant influence over the direction of decision making on key data protection cases if it is unable to take part in the European Data Protection Board, the EU group of data protection authorities under the GDPR. The board can take binding decisions and there is a risk of losing influence in precedent setting cases involving online platforms under the GDPR, on areas such as profiling and the right to be forgotten. A bespoke agreement should also aim for the Commissioner to retain her position on the Board.

In August 2017 the Government set out its position on the future data protection relationship with the EU. The Commissioner supports the partnership paper and is working closely with the Government to provide expert advice on the practicalities of any new partnership.

16 May 2018

[849] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-home-affairs-subcommittee/eu-data-protection-package/oral/48744.html

[850] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/exiting-the-european-union-committee/the-progress-of-the-uks-negotiations-on-eu-withdrawal/oral/82783.html

Information Commissioner's Office – oral evidence (QQ 113-121)

Tuesday 11 September 2018

Watch the meeting

Members present: Lord Gilbert of Panteg (Chairman); Lord Allen of Kensington; Baroness Benjamin; Baroness Bertin; Baroness Bonham-Carter of Yarnbury; The Bishop of Chelmsford; Lord Goodlad; Lord Gordon of Strathblane.

Evidence Session No. 13 Heard in Public Questions 113-121

Examination of witness

Elizabeth Denham, Information Commissioner, Information Commissioner's Office (ICO).

Q113 **The Chairman:** I am very happy to welcome Elizabeth Denham, the Information Commissioner, to this evidence session of our inquiry into regulation of the internet. Commissioner, thank you for your time and for being with us this afternoon. I will ask you to say a few words of introduction in a moment. I remind members of the Committee to declare any relevant interests at an appropriate point. I would like to make a declaration myself. I worked for the group Britain Stronger in Europe during the campaign to remain in the EU before the 2016 referendum and I was consultant to the Conservative Party at the last general election campaign. Both these organisations have been of interest to the Commissioner with respect to the use of personal data during those campaigns. The activities have not been the subject of this Committee's inquiry and I do not anticipate that they will be at issue today. I have not personally been the subject of any requests from the Commissioner and I no longer have any role with either Britain Stronger in Europe or for the Conservative Party other than party membership. I make this declaration for the sake of full disclosure.

Commissioner, thank you again for your time. I hope you have been following our inquiry, which is broad in nature, into the future regulation of the internet. One of the areas that we are particularly interested in is how to have a horizon-scanning approach so that we are not just reacting to issues that cause public concern but have a public policy-making approach that is abreast of issues as they develop, as technology develops and work in the area becomes of public interest. We would like to discuss that with you at some point. Today's session will be recorded and a transcript will be taken.

Commissioner, can you start by describing the current role of your office—its role in the online regulatory framework—and tell us a little bit about your resources, the challenges of doing your work within those resources and whether they are sufficient for the role that you undertake?

***Elizabeth Denham*:** Thank you very much for the invitation to be here to discuss these issues with you. It is an interesting inquiry. As the UK's regulator for data protection, my office has a crucial role in the regulation of activities on the internet as they relate to personal data. As we know, personal data underpins so much of the commercial activities that are happening online. We definitely have a horizontal role across all industries.

The ICO regulates 11 pieces of legislation and includes the general data protection regulation, the Data Protection Act 2018 and the Freedom of Information Act as well. We are already a regulator that is well versed in balancing openness generally, certainly on the internet, with the private space in the public interest. We are very much engaged in these activities. Many of the activities—the elements of the internet—are regulated. You have heard that from many of the witnesses who have appeared before you. We do not think that it is the Wild West. It is regulated, and personal data that underpins so much of the digital economy has just been given a once-in-a-generation reboot regarding the powers of the regulator, the increase in our jurisdictional reach, sanctions against companies that break the law but also new rights for consumers and citizens.

Whether you are talking about the greengrocer or Google, these activities involve citizens' data online or offline and they are already regulated. One way of thinking about it is that data protection is medium-blind. From online harms, which you have been discussing, to legal and illegal content, fake news to data monopolies, data interoperability and the responsibilities of the tech giants, these are broad and complex issues and data protection is a thread that runs throughout.

One thing that is clear to me and which is clear to many commentators in the public is that things cannot continue the way that they are. The time has come to have more rules and more controls for individuals to protect against some of the harms that are of deep public concern.

When it comes to data protection law, maybe in comparison to other areas of regulation our law in the UK is world leading and, because it has just had a reboot, it is fit for purpose for the digital age. When we are undertaking reviews of regulating activities on the internet, it is right that we look deeply at the types of harms, identify them clearly, look at the existing levels of regulation and the reach of regulators, look at the gaps and then, only after that analysis, decide whether there needs to be a new regulator or new regulations. This kind of deep inquiry and consultation is really important.

You wanted to ask me whether I had the resources to do the job. If you had asked me that question a year ago I would have had a different answer. I think the law is fit for purpose for the digital age. The Government have given me, effective from January, a pay flexibility that allows me to better recruit experts, especially technical experts and legal experts to help me with my work, and the Government have also provided a new fee regime for the ICO. Our budget has gone up 58% since last year and that allows us to do some of the work that we really need to do. A year ago, however, I would have had a different answer.

The Chairman: Could I ask you a little bit more about that? You have the resources to attract the kind of expertise you need. Presumably you are competing with tech businesses in many cases to attract recruits. Is there a skills shortage and are there sufficient people out there, regardless of whether or not you have the resources to fund them?

***Elizabeth Denham*:** It is helpful that we have pay flexibility and we have the resources to be able to attract them but there is a skills shortage out there. What we have to offer is perhaps different from what tech companies have to offer. We are doing socially relevant work. We have secondment programmes that bring people in from the private sector and the technology sector. We have an academic fellowship where we have just attracted an expert on AI to help us with setting up our programme for auditing algorithms. We are trying to reach into the private sector and trying to do what we can, but I agree that there is a skills shortage in this area. If you look at one of the hot jobs now in the jobs pages, it is data protection officer. It used to be a back-room area of practice but is definitely a front-burner now. We are competing therefore with large companies and technologists.

The Chairman: You said, as indeed did many of our witnesses from across the industry, that we have world-leading regulation in this country and that that applies to your organisation and fellow regulators. That is world-leading with regard to the quality of the regulation itself, but what role do you play with international regulators? How do you demonstrate that global leadership?

***Elizabeth Denham*:** With our European counterparts and colleagues, we are part of the European Data Protection Board and we have led in 40% of all the guidelines that have been written to interpret the GDPR. We are collaborating on enforcement and policy work not just with our European colleagues but with international players. The ICO is a member of the Common Thread Network, which is a connection of Commonwealth countries. We are a participant and leader in the Global Privacy Enforcement Network, which has over 50 regulators around the world. We work with the Federal Trade Commission under the terms of a memorandum of understanding. We are globally connected and that work needs to continue after exiting the European Union. It will be very important that the ICO continues to play a role. We are the largest data protection regulator in the world in terms of resources and numbers. We are now leading an investigation that has the interests of all the players in the world into political campaigns and the use of data analytics. The world is watching this investigation.

The Chairman: Thank you. We may well come back to the international dimension. Baroness Bonham-Carter.

Baroness Bonham-Carter of Yarnbury: May I pick up on the enforcement point? We are talking about big companies. Do some respond to fines or whatever by just shrugging their shoulders and putting it down to a business expense?

Elizabeth Denham: In the previous regime, when our fining power was a maximum of £500,000, that might have been true, but with our new fining powers of up to 4% of global turnover it is much more significant. In fact, with the big global companies it is not even the fine that will have them concerned but the hit to the reputation and the loss in users' trust of platforms if a regulator imposes a fine for contravention of the law. You will know that we have issued our notice of intent against Facebook for the maximum fine under the old regime and we will be settling that issue fairly soon.

Q114 **Lord Gordon of Strathblane:** Various witnesses in written evidence have pointed to the number of different organisations in Britain regulating the internet to some degree or another and said that this could be confusing. What is the best way of handling this? Could we have a co-ordinating body that makes sure that they are all singing from the same hymn sheet on principles at least, or do we need a meta-regulator standing above all of them?

Elizabeth Denham: Ultimately, it is for Parliament and policymakers to decide how many regulators there should be and what they are responsible for. Let me tell you what we do right now. Because the ICO has a horizontal reach across all the activities on the internet, we work with industry regulators very closely. We are working with the FCA, for example, on a very similar sandbox initiative so that we are looking at fintech projects that the FCA is looking at in some of the same ways. We have seconded someone from the FCA to help us build our sandbox. We are working with Ofcom. In a week or so we will be releasing research that we have co-operated and collaborated on. We have worked with the Electoral Commission on some of the policy recommendations. It is not ad hoc.

Lord Gordon of Strathblane: And with regard to standards, presumably you liaise with them. Do you think it needs a separate body or can it be done by harmonised co-operation?

Elizabeth Denham: We have harmonised co-operation, but it is probably not well known how much work is done under the covers. There would be a role for a co-ordinating body that is forward looking—not reactive but proactive and identifying future gaps in the law and assisting the regulators in getting the resources that they need. Maybe there are law changes that need to happen because this is not a static area. It is moving very quickly.

I like the idea of a co-ordinating body. There is a new body in town called the Center for Data Innovation and maybe there is a fit for a body like that to draw things together. The last comment I will make is that the economic regulators are getting together to look at whether or not there is a harmonised or consistent way that we can look at algorithmic bias and algorithmic transparency. There is a lot of work to do.

Q115 **Lord Goodlad:** I want to ask about data protection law being described as principles-based, being based as it is on the data protection principles. In your view, what are the advantages and disadvantages of using principles-based regulation?

Elizabeth Denham: Principles-based regulation works for an area of law that is fast changing and fast moving. The principles-based legislation, which data protection law is, allows for more detail to be developed through guidelines, codes of practice and certification that flow from the principles. Some commercial entities like more prescriptive or rules-based legislation because there is certainty, but it is not very flexible; it is rigid and it is not future-focused. One example is that in data protection law there is only one principle about data security. It says that organisations have to have appropriate safeguards in place to protect against misuse and unauthorised access. The question we always get is: what is appropriate? From there it is context that you have to look at. How sensitive is the data? What are the threats and risks on the horizon? If the law said that everybody had to have 256-bit encryption, that would be outdated. What is appropriate, therefore, is going to change depending on the environment. That said, we get many complaints from companies that say, “Just tell us what ‘good’ looks like. Just tell us what we are supposed to do". The beauty of the GDPR is that it provides for codes of conduct and certification and co-regulation in specific areas of practice.

The Chairman: To follow through on the principles-based regulation, you talked about how we need to be forward looking, which means applying those principles to risks as they develop and presumably applying solutions as new solutions become available. Who in this mix is responsible for that broad, forward-looking approach for scanning the horizon, identifying future risks, future technological developments, changes in behaviour in tech companies, different remediations and what might be happening around the world? This is not just about data; it is about a whole range of regulatory approaches. Who in the mix is responsible for that?

Elizabeth Denham: There is not one regulator or one authority that is looking that far to the horizon. We are doing that work in data protection but are not necessarily looking at changes in consumer attitudes or behavioural changes or new societal risks or ethical considerations. That is not the job of the data protection regulator. You talked about a co-ordinating body—a body that is looking to the future. That is maybe a solution that we need to look for in the UK.

The Chairman: You do not seem to be formally advocating such a body, but is it a possible solution that might work across regulators?

Elizabeth Denham: It could do and you would have to have a lot of different types of expertise on a body like that. Societal attitudes change. I sense a change in consumer concern over hacks on the internet, over data protection issues, over profiling and targeting in a way that was not there three years ago. Watching for these societal concerns and changes, while it is for Parliament, there could also be an expert body.

Q116 **Baroness Bertin:** I would like to declare an interest. I work for BT. I want to bring you back to some of your comments in your introduction about harm from the internet and particularly to talk about ethical design and what principles you think should underpin ethical design.

Elizabeth Denham: From where I sit, I am hearing that people are more and more concerned about both illegal content on the internet and legal content where it does not quite reach the threshold of a criminal act. There is concern about that. One of the designs that we need for the internet is protection against illegal content and offensive content, especially when it comes to children and vulnerable adults. Any kind of internet design needs to take that into account.

Baroness Bertin: Some of our witnesses have said that in truth designers are not going to ethically design unless they are forced to. Would you agree with that analysis?

Elizabeth Denham: I think that is right. One of the interesting tasks that we have been given at the ICO from the Data Protection Act 2018 is that we have to develop a code for age-appropriate design. This is a really interesting task because we are looking at the standards of design for kids' websites and games and how companies are going to have to comply with that. We are doing a consultation now to come up with that kind of design. That is going to be unique. That code is unique in the UK and not a requirement anywhere else.

Baroness Bertin: Have businesses been involved in that consultation? Are they running towards it or not?

Elizabeth Denham: The big companies are not necessarily running towards it but they do know that there are special obligations they have to protect children online when it comes to consent and content. That goes back to design. Another principle for the ethical design of internet activities is that people should have the same rights online as they have offline. I am not saying that regulation can be copied and pasted over to the online world but I do think that people should have the same rights.

Q117 **Lord Allen of Kensington:** I am interested in three things. What challenges have you faced implementing the Data Protection Act 2018? Secondly, what are the lessons learned? Thirdly, have there been any common themes? I am trying to get a feel for the level of intervention. Is there a common theme in regard to what has taken up your team’s time in the past year?

Elizabeth Denham: Our initial challenge was getting organisations engaged in getting ready for the obligations under the Act. What helped there and focused the attention of organisations on their new responsibilities was the level of the fines. Even though we had data protection law for 20 years in this country it almost felt as if most companies just woke up to their data protection responsibilities when they saw the fines. Data protection becomes a boardroom issue. It becomes a risk issue for senior executives. We spent a lot of time in the last two years both myth-busting about what the Act really required but also helping to ensure that data protection was baked in to the business practices of organisations and not just bolted on in the department of legal compliance. At the end of the day, if personal data is the most important asset that a lot of organisations have, they have to have strong data governance and legal compliance. That was the first challenge—getting the attention of the board.

Lord Allen of Kensington: To specifically pick up on that, the Centre for Policy Studies told us that there was widespread confusion. Do you think that we are through that now? Do you think that there is still confusion in businesses about what we need to do, or is that going to take a number of years?

Elizabeth Denham: We spent a lot of time on guidance and every industry sector wanted their own specific guidance. We have 5 million businesses across the UK and all the public bodies and their special issues and we did what we could. The other challenge was small businesses. Micro-businesses and small businesses were concerned about the new obligations on them and how to identify risks and build in the measures that they needed to. We did a lot of work with industry associations representing small businesses. We had a whole stream of work around small agencies.

There were two other challenges. One was the demand for the expertise of our staff. At one point we lost 25% of our expert staff to other companies that could pay more and attract them. That was a huge impact on the ICO. We might be over that now. The other issue was that we underestimated the exercise of rights. Individuals have come to our office well beyond our estimation. We thought we might have a 30% or 50% increase in complaints and calls and inquiries. It was 100% increase in the first three months under the GDPR. It is crunch time for us to be able to deal with those front-facing services.

Lord Allen of Kensington: What types of incidents have taken up most of your time?

Elizabeth Denham: A lot our time is spent dealing with data breaches. Data breaches and incidents of a significant nature now have to be reported to our office and we had to deal with thousands of those complaints in the first few months. That is liaising with the companies, giving them advice and deciding if we are taking enforcement action, data breach notification incidents and education of various sectors.

The Chairman: You have seen a significant increase in the number of complaints from consumers and from the public. Presumably, you have an investigative threshold by which you determine whether a complaint reaches that threshold for investigation. Do you have any stats on the proportion of complaints that are meeting that threshold?

Elizabeth Denham: Our general process is to require the individual to take their complaint to the organisation first, and only when they are not satisfied with that response they come to us. We get a lot of complaints where people have not taken a complaint to the company or the public body, so those go back and we take the complaints after that. I can write to you and give you a better sense of the numbers that are coming in, which ones we are accepting and even which industry sectors or government agencies they are coming from.

The Chairman: That would be useful if you could write to us. Thank you.

Elizabeth Denham: There has been a 100% increase.

The Chairman: Is your impression that any of those are vexatious or not meeting the threshold and not sufficiently evidenced?

Elizabeth Denham: I think that people have woken up to their data protection rights. We ran a public education campaign called Your Data Matters. That might have been quite successful, but I also think that people are filing more requests to get access to their own personal information. There have been requests for porting data under the new data portability rights. There have been requests for de-linking and removal and deletion of information under their right of erasure.

Lord Gordon of Strathblane: May I suggest something that might save some work? As you allude to in your evidence, most people do not know the terms and conditions that they are signing up to. I freely confess that I am so concerned to put my large finger on the right very small button on my iPhone agreeing to terms and conditions that I do not read them. Would there be a case for your organisation issuing a kitemark, approved stamp of approval, on recommendations so that people know it is safe enough to sign up for this because we all know that nobody is going to read them all?

Elizabeth Denham: That is a great question because I think hardly anybody is reading terms and conditions and there is a lot of fatigue in that approach. The GDPR gives us the ability to certify and to develop kitemarks. That is the next stage of the work that we need to do. I agree with you that people almost need a symbol to be able to identify what is safe and what is not. That will come out of the age-appropriate design code. To start thinking for kids, there almost needs to be a traffic light system.

Q118 **The Lord Bishop of Chelmsford:** I want to ask about algorithms. In what ways do you think algorithms could and should be accountable, fair and transparent? I can say a bit more about what lies behind the question if you need it, but hopefully that will not be necessary.

Elizabeth Denham: One of the reasons that the EU Directive 95 became the GDPR is that there was a lot of public concern about black box algorithms and opaque decision making by machines. A lot of the new rights in the GDPR, therefore, are about algorithmic accountability, about explicability and giving the regulator new powers to audit algorithms for fairness and for transparency. That piece of work is very new to us. If you are asking me how algorithms can be transparent, however, there are different levels of transparency. Consumers need one level. They do not need computer code. They need simple explanations about the algorithms that are at play and, legally, if significant decisions are made by machines with no human intervention they have a right to an explanation.

Another level of transparency is to the regulator. It is for our office and maybe other economic regulators to go in and find out what data goes in, what questions were asked and what are the decisions that come out. That is another layer of oversight. It is not the same as transparency to the people.

The Lord Bishop of Chelmsford: Do you think that the framework that you now have with the GDPR is sufficient for doing this or would you be looking and hoping for more?

Elizabeth Denham: There may be a gap. The law might sound better than it actually is because it gives the right of explanation to individuals for decisions that are made solely by machines. The wording of the legislation might therefore be problematic. We need time, however, to let the law bed in and to have some cases and to do some guidance and some auditing. The ICO is working with the Alan Turing Institute on a tool for algorithmic transparency and algorithmic auditing. This is a new space for regulators to be in. If there is anything we can do as regulators it is to harmonise our approach to how we are going to look at machine decision making.

Q119 **The Lord Bishop of Chelmsford:** Forgive me if I was not listening carefully to your answer to the previous question. I was not quite sure if we got an answer to the last bit of the question, but I may have just dropped off for a moment. I was interested in hearing, particularly in relation to this, what the initial lessons are that you have learned from the introduction of the GDPR, because it seems to me that, looking at it not so much with my House of Lords hat on but with my mitre in place as the Bishop of Chelmsford, for the 600 parishes that I serve the anxiety levels were enormously high about things such as, "Do we have to delete our Christmas card list, Bishop?". Now that we have gone through to the other side, I am noticing a huge increase in awareness of these issues, which seems very positive. People's understanding of the world that they have been inhabiting for a while has increased hugely. I think it is the GDPR which to a large extent has done that. It would be interesting, therefore, to hear you reflect more generally on this. The next question might be, as people's expectations are also increasing, how you are going to help them.

Elizabeth Denham: You are right. No pressure for us. There is nothing like a new law to focus everybody's attention, especially a new law with large sanctions—not just fines but also new powers of the regulator that we can order a company to stop processing personal data. This can have more impact than a fine at the end of the day when you think about business models.

Yes, it has focused the attention of companies and public bodies. All kinds of charities are focused on this, with marketing and profiling. I did not like the anxiety, but we kept saying that GDPR was not the Y2K of 2018. It is the beginning of new awareness and better systems in place to take care of people's data. The other thing that is unfortunate is that there were a lot of consultancies that got involved in this and a lot of scaremongering. That is where we had to do a lot of literal myth-busting to say that the GDPR is not all about fines and here is your basic responsibility. If you are a micro-business and you are a butcher on the corner you are probably not going to be impacted by the GDPR.

On lessons learned, I guess we could have tried harder to bust some of those myths earlier, but we had to get the attention of organisations to do that. We also did not have the capacity to go out and educate every business and every sector.

Baroness Bonham-Carter of Yarnbury: Going back to the algorithms and the risks they pose, one of the things that has come up a lot in evidence given to us so far is the targeting, or micro-targeting, particularly of those with addiction problems and so on. As with the Bishop, you may have answered this in your previous answer, but do you think we have sufficient powers to combat this?

Elizabeth Denham: Yes, we issued a report in July called *Democracy Disrupted?*. That report and our investigation is about the use of data analytics to micro-target voters in campaigns and elections. I would point you to that report because there is a series of policy recommendations in it about improvements that we need in the law. The purpose of the report was to pull back the curtain to show citizens how their data is used in a campaign or a referendum. We are investigating 30 different organisations, from political parties to social media companies to data analytics and political consultancies, to unpack what that ecosystem looks like and why you would get a certain message where that data comes from—data brokers, et cetera. We have taken action against some of those organisations. We cannot do everything under data protection law because there are ethical issues for government, for Parliament and for policymakers to look at, but we are pushing the envelope on that in our large investigation and that is the one that has the attention of the world.

Lord Gordon of Strathblane: The problem is that it is sometimes impossible to trace the source of the intervention. Is the answer perhaps to target the messenger rather than the message and insist that anyone putting something up has to have a real address and be a real person and not a robot and have some process of rectifying the wrong if they have done something wrong?

Elizabeth Denham: Are you talking about anonymity on the internet?

Lord Gordon of Strathblane: Yes, I think that there are issues. Obviously there are arguments on both sides. Some people would not intervene at all if they did not have the guarantee of anonymity but equally I am sure that you would agree that it can frequently be abused.

Elizabeth Denham: That is why I think your job is so difficult.

Lord Gordon of Strathblane: That is why we are asking you to help us.

Elizabeth Denham: You are trying to balance the private space with openness and transparency. If you take a political campaign, for example, everybody agrees, Facebook, Twitter, Google as well, that the source of political advertising should be imprinted. It should be marked and people should know where that ad is coming from. That seems to be easy as opposed to identifying an individual on the internet and what the outcome is of that. These are challenging questions and it will take time for us to map them and identify the significant harms.

Q120 **Baroness Bonham-Carter of Yarnbury:** I want to come to platform dominance. In your written evidence and in what you have said already today you make it clear that you are concerned about data monopolies. Could the implementation of uniform standards and data portability mitigate what you see as the negative consequences?

Elizabeth Denham: It can help. Data portability is a new right which allows individuals to port their data from one service provider to another. We can see how that might build better innovation and market share so we understand that. It also gives people control. I am concerned about data monopolies, however, when you see for example the spend of political campaigns that goes towards online political advertising, mostly through Facebook, and you think about all of that data in the hands of one company. I worry about data hacks, hacking into a database, and the lack of innovation. I think that is what people are really concerned about, too.

The other thing about data monopolies is that we intervened in a case when Facebook purchased WhatsApp. The purpose of that merger was to share more data. So many mergers and acquisitions that are happening in the market are really about data and consolidating more and more personal data in the hands of the company. In that case, with Facebook and WhatsApp we were able to get WhatsApp to sign a commitment that data sharing would not take place until they could prove to us that it would be legal. Competition law can probably look at some of these issues, but data portability and standards can help.

The Lord Bishop of Chelmsford: Did they prove it was legal?

Elizabeth Denham: No, we are still waiting. Those are the kinds of issues where you see more and more mergers, which are really about getting more data and compiling more data and profiling more people in the commercial sector.

Baroness Bonham-Carter of Yarnbury: You are now fighting it.

Elizabeth Denham: We have not had any more moves from Facebook and WhatsApp on their sharing of that particular data.

Q121 **Lord Goodlad:** I have two questions. First, what are the problems of enforcing UK regulations on companies based outside the jurisdiction of the European Union—the United States of America being the obvious example—and how are these problems were overcome? Secondly, what effect do you think this country leaving the European Union will have on the overall regulation of the internet?

Elizabeth Denham: How do we enforce UK law outside the bounds of the United Kingdom? We are involved in several cases where we are taking action against companies that are located elsewhere. I will give you one example. In the Cambridge Analytica/Facebook investigation, one of the companies we are investigating, AggregateIQ, is based in Canada. It was involved in the referendum campaign. We are using the help of our Canadian colleagues through a memorandum of understanding to obtain the information that we need to take action. We have the help of our Canadian colleagues, but the actual enforcement of the law is a challenge. How would we actually carry out an enforcement notice against a Canadian company? That is an open question for us right now. We have taken action against some US-based companies that are associated with UK companies, and by contract the UK regulator has a right to investigate and enforce the law. You will see my decision next week that will make this answer a little less vague. That is by contract.

The GDPR has extraterritorial reach, so it captures the data of EU citizens processed by companies outside the EU. The actual enforcement of the GDPR, however, needs to be given some practical experience and I believe it is going to need bilateral agreements and mutual legal aid treaties—MLATs—to make it real. We are at a very early stage right now.

Lord Goodlad: So it is a big challenge and a big problem.

Elizabeth Denham: It is a big challenge. We will see how practical the extraterritorial reach of the GDPR actually turns out to be in the enforcement. Your second question was about the impact on enforcing the UK law if we are no longer in the European Union. The ICO is a member of the European Data Protection Board, so we have the EU 27 as a strong contingent of enforcement action. If we are no longer part of the board, the UK will be on its own enforcing a similar law but without the co-operation, consistency and mechanisms of the board. If we are not part of the board and there is no data arrangement that keeps us in that enforcement club, we will be turning to bilateral agreements with data protection agencies to do joint enforcement.

Lord Goodlad: Have they been involved in any discussions about this possible eventuality?

Elizabeth Denham: I have been talking to my European colleagues about the eventuality of a different relationship and what that would mean. I know many of my colleagues would be willing to jointly enforce with us. That is very future focused, however, because we do not know what our relationship is going to be right now. It is one for the Government.

Lord Goodlad: Have you talked to the British Government about it?

Elizabeth Denham: I have. I have advised government and been consulted by government on the impact of enforcement if we are no longer a member of the board or part of the European Union.

Lord Goodlad: How has that discussion been reflected?

Elizabeth Denham: In the Government's partnership paper. The Government's ambition is for an arrangement beyond adequacy that keeps the

ICO as a member of the European Data Protection Board. If that does not happen we will have to look at bilateral agreements to jointly enforce. There are member states where there is a higher risk to UK citizens where the data is flowing. That is where I would go. My mandate is to protect the data of UK citizens and I will do whatever I can to have those arrangements in place. I agree with the Government, however, that the best-case scenario is an ambitious data deal that keeps us very close to the Europeans, not just in law but also with joint enforcement. The weather is going to be made in the EU on these big internet cases.

Baroness Benjamin: There is a TED talk by James Bridle, which has had nearly 3 million viewings, called *The nightmare videos of children's YouTube—what's wrong with the internet today*. A lot of the videos that children are watching are not only inappropriate in many ways because of the content but also extremely addictive. I would like therefore to ask you, out of those 3 million people, especially parents, who want to complain but do not know who to complain to, have you had any complaints about this particular part of the internet where children are being attracted to watch inappropriate material? Is this something that Ofcom or maybe the BBFC should be regulating or do we need a new regulator to look at this kind of issue? Do you feel that the regulation of YouTube and other platforms should be the same as for terrestrial broadcasters?

Elizabeth Denham: I am not a content regulator. I do agree with you that in the kind of research we have done with Ofcom about the harms that people are concerned about on the internet, one concern is about children and what they are able to view online, including videos and other sites. A complaint about the content of a video would not come to our office, but I do agree that people do not know where to take their complaints. They might ask YouTube to take the video down, but that kind of issue and complaint is probably better examined by an organisation such as the BBFC, along with some of the filtering and identity. When it comes to addiction online, that is another harm that needs to be carefully identified and scrutinised, but it is not directly a data protection harm. Whether we will be considering some of these issues in our age-appropriate design code I do not know. I am sure that we are going to hear about that in our submissions.

Baroness Benjamin: Do you feel that the organisations that you have already mentioned should all be working together to deal with this type of material, which is online, because there is a world out there that parents do not know how to navigate? Everybody should be getting together because, as far as James Bridle is concerned, we all need to work together to stop children being exposed to online material like this. What would your role be if you had to be part of the bigger conversation?

Elizabeth Denham: If it is part of a bigger conversation, it needs to be because you are talking about many things here, including content regulation, the role of parents and the role of internet companies. It is a conversation that is going on right now. This inquiry is part of that conversation. My response would be that there needs to be a clear inventory of what the harms are, the extent of the existing regulators, what activities they cover, what actors they cover and whether they can reach into other jurisdictions to have an impact, because many of these companies are based elsewhere. All of these things are important. Only then can you decide whether you need to create a new regulator or add to the remit of the existing regulators.

Baroness Benjamin: They are looking to see how many times the children are pressing the button to look at this material and using it for advertising. It seems to be a link that we have to get our heads around to say that you cannot show that type of thing in order to gain advertising in order to get on to a platform to get to children. It is a sneaky way of getting to children which 3 million people feel is completely inappropriate.

The Chairman: Who would be the lead regulator on the aspect that Baroness Benjamin describes?

Elizabeth Denham: That is a complex set of questions because you are talking about content and also about the use of personal data to target advertising, so that would be my role.

Baroness Benjamin: That is the main thing he was pointing out. The content is just part of it. It is the advertising and getting to the children that people feel is unsatisfactory and somebody should be looking at this because of when the children become teenagers and adults. Eighteen month-old children are getting hooked because of the kind of behaviour that is online. What are we going to do about it? I thought I would ask that question to see where you stand and what you feel that we as a Committee should be doing and looking at.

Elizabeth Denham: There is no silver bullet to say here is the answer, that it should be the ASA and Ofcom and the ISO and industry codes of practice and it should be independently regulated. Those are numerous questions. We are involved when personal data is used to deliver content or deliver advertising. We can look to see whether it was used fairly. For the first time in law in the GDPR, children are treated differently: there have to be special arrangements for children both in terms of the use of data analytics and algorithms but also the form of consent and the use of sensitive data. Children are treated specially for the first time in law in the GDPR. This Committee might look at that, because I do not think it exists in the other laws and regulations. You need another regulator that is deciding to filter certain content or tag it as acceptable or not.

Baroness Benjamin: Could I ask you to look at that video by James Bridle, the TED Talk?

The Chairman: We have taken note of the video you are referring to.

Lord Gordon of Strathblane: I was just wondering, slightly off subject again, whether there is a danger of conflict between the British approach to law and the American approach to law. It has been alleged in written evidence to us that Twitter would disregard a UK court order unless they got a similar one from a United States court. That is an allegation that we will put to Twitter later in the afternoon, I imagine, but is the difference between American law and British and European law a problem?

Elizabeth Denham: I am not a legal expert in all of these different areas of regulation but, generally speaking, the US is looking at the standards in Europe because they have to look at compliance in a different way because of the jurisdictional reach of the GDPR. For the first time after Cambridge Analytica and Facebook and how data was used during the 2016 presidential campaign, they are looking at these other standards. At the end of the day the approach in the UK has to reflect our cultural values. That is what it is all about. The challenge is that the internet knows no boundaries. Geopolitically the internet does not see that. How do you make sure that British law is respected when you are dealing with large American companies? It is a challenge.

Lord Allen of Kensington: You have talked about a super-regulator—Ofcom, CMA, ASA, FCA or whatever. Have you identified anything that is falling between the cracks? You know what you are looking at. Ofcom is very clear about what it is looking at. I would be interested to know if there is something that is falling between the cracks and, if there is, what we would do about it. There was a suggestion earlier of some sort of co-ordinating body that gets everyone working together.

Elizabeth Denham: There are two things that are falling between the cracks. Although we have defined what illegal content is, people are really concerned that it is not properly enforced online. How do you enforce our standards? If there is illegal content, how do you get it down without depending on companies to be the judge and jury in whether to take that off? When it comes to legal content, where it is legal for the content to be online but it is intrusive or disturbs people or harasses people and does not meet the standard of illegality, who is going to make the determination that that information needs to be taken down or censored in some way? Who makes that decision? That is where you might look at some kind of an ombudsman or an intermediary. You need codes of conduct that are created, certified and backed up by an independent regulator. The space that everyone is grappling with is things such as what do you do with the legal content without leaving it in the hands of the big companies or the platforms. We know they are not just benign platforms any more, but what is their responsibility and liability?

The Chairman: Thank you very much for your evidence, which has been very impressive and informative for the Committee. Thank you also for the written evidence that you sent us. We have had a very interesting discussion about the possible need for an overview across the regulatory piece and some of the potential gaps that you have identified, some of which Parliament may feel are not being addressed by regulators. It may well be that as we develop our thinking on that we may want to come back and talk to you further. Your evidence in that area has been very interesting, as has all of your evidence. Thank you for your time today.

Information Commissioner’s Office (ICO) – supplementary written evidence (IRN0120)

I would firstly like to thank the Committee for the opportunity to give oral evidence to your inquiry on the regulation of the internet on 11 September 2018. This is an important and timely debate and one in which the ICO wants to play its full part.

During my evidence session I explained that my Office had seen a significant increase in the number of complaints being received from members of the public about potential breaches of their data protection rights since the GDPR came into force in May 2018. I agreed to provide you with the most up to date figures we hold on the number of complaints the ICO has received in the period since May 2018 compared to the same period last year and a breakdown of the top ten sectors against which these complaints are made. These are contained in the attached annex.

It may be worth explaining that the GDPR provides the right to make a complaint to a Supervisory Authority, like the ICO, if someone believes their rights have been infringed (Art 80). A Supervisory Authority is required to handle these complaints and investigate “to the extent appropriate” and inform the complainant of the progress and outcome of the investigation (Art 57).

Therefore, as such there isn’t a threshold which would limit the number of cases that require a response from the ICO. The extent to which we will “investigate” or review a complaint depends on a number of factors including the seriousness of the issues raised, the categories of personal data affected including sensitive personal data and the information provided to us when the complaint is made. Ultimately, all complaints demand a response from my office.

In addition, the ICO’s Regulatory Action Policy851, which was considered on 11 September 2018 by the House of Lords Secondary Legislation Scrutiny Committee, details our risk based approach to taking regulatory action against organisations and individuals that have breached the law in relation to data protection and freedom of information.

The ICO’s new funding model came into effect at the beginning of this financial year. This together with new pay flexibility from Government means that the ICO has more capacity and flexibility to deal with the increase in demand for our services and our additional responsibilities under the new data protection regime. We will of course advise Government and Parliament if this situation changes or if more capacity is required.

I hope this information is useful to the Committee. If I can be of further assistance to the Committee’s inquiry into internet regulation, please do not hesitate to get in touch.

26 September 2018

[851] https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf

ANNEX

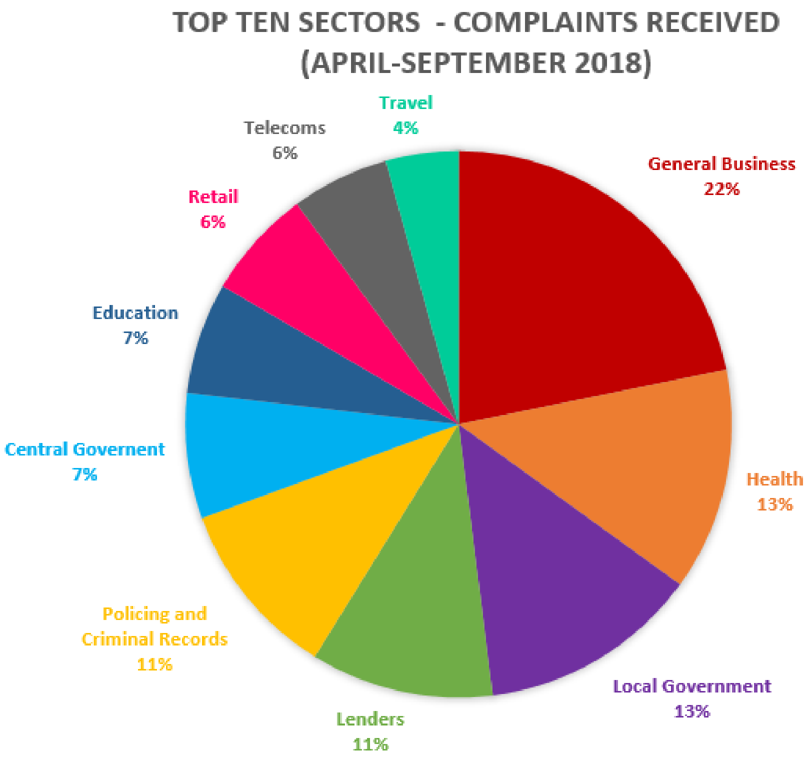
Fig.1

			Complaints Received
2018-19	Q1	April	2,162
		May	2,309
		June	3,070
	Q2	July	4,173
		August	4,376
Total			**16,090**

Fig. 2

			Complaints Received
2017-18	Q1	April	1,429
		May	1,727
		June	1,634
	Q2	July	1,744
		August	1,838
Total			**8,372**

Fig. 3



Information Law and Policy Centre, Institute for Advanced Legal Studies – written evidence (IRN0063)

Submission Summary

The Information Law and Policy Centre (ILPC) is a research centre within the Institute for Advanced Legal Studies, School of Advanced Study, University of London. The Centre is focused on promoting, undertaking and facilitating cross-disciplinary scholarship and research in the broad area of information law and policy, both domestically and internationally.

This submission from the ILPC is in response to the recent call for evidence on 'The Internet: To Regulate or Not to Regulate' from the House of Lords Select Committee on Communications and outlines four key issues:

1. Whether Internet regulation could do more to enhance the protection of human rights?;
2. Protecting freedom of expression;
3. The use of deceased's data (in response to Question 6 of the call to evidence: What information should online platforms provide to users about the use of their personal data?); and
4. The role of the UK as a world leader in Internet regulation

List of contributors

Dr Nóra Ni Loideain, Director of the Information Law and Policy Centre and Lecturer in Law, Institute of Advanced Legal Studies, University of London; Visiting Lecturer in Law, King's College London; Associate Fellow, Leverhulme Centre for the Future of Intelligence (CFI), University of Cambridge.

Professor Lorna Woods, Professor of Law University of Essex, and Senior Associate Research Fellow, Information Law and Policy Centre.

Dr Edina Harbinja, Senior Lecturer in Law, University of Hertfordshire.

Dr Rachel Adams, Early Career Researcher, Information Law and Policy Centre, University of London and Research Associate, Human Sciences Research Council, South Africa.

1. Whether Internet regulation could do more to enhance the protection of human rights?[852]

1.1. Any future legislation governing the Internet and any new or emerging technologies or practice that interferes with human rights (e.g. freedom of expression, due process, prohibition of discrimination), such as algorithms developed to track facial recognition within CCTV systems, should contain explicit provisions that mandate an in-depth, evidence-based, and independent evaluation of the operation of such measures, and specifically their compatibility with human rights law.[853]

1.2. Provisions currently exist for this due diligence to be undertaken in the case of assessing data protection implications in the form of 'Data Protection Impact Assessments' under s.64 of the Data Protection Bill 2017 *prior to the use of such systems* (the processing stage). However, it is submitted that this assessment must take place earlier in order to be in any way effective in practice.

1.3. Also, limiting the scope of assessment to the impact on data protection does not go far enough in terms of adequately assessing the risks posed by emerging Internet-based technologies for other collective public interests within a democratic society, such as the rule of law and the integrity of elections. Hence, there is a need for a robust approach to human rights due diligence and good governance in the form of a legislative requirement for '***Human Rights Impact Assessments***'.

1.4. Those with the qualifications, knowledge, and experience of applying such legal standards, that is to say the *legal departments/legal officers*, within the relevant industries and public bodies should be required to undertake such assessments *during the development of such systems*. Furthermore, it is crucial that this due diligence is undertaken at this stage of the technical process in order to inform and guide the work of the front-line professionals who are responsible for the design and future maintenance of these systems.

1.5. Otherwise, as highlighted in the recent House of Lords Report on Artificial Intelligence (AI),[854] attempting to retrofit such legal standards (such as 'explainability', which is derived from the long-established legality principles of accessibility and foreseeability under the Human Rights Act 1998) into a complex and sophisticated AI-driven system that has already been implemented is either incredibly difficult or impossible.

1.6. This due diligence and good governance will serve to ensure that such laws are implemented in ways that respect and comply with key human rights principles and the related conditions of legality, necessity, and proportionality, as guaranteed under the Human Rights Act 1998 and European human rights law

[852] Section author: Dr Nóra Ni Loideain.

[853] N. Ni Loideain, 'Cape Town as a Smart and Safe City: Implications for Privacy and Data Protection' (2017) 7(4) *International Data Privacy Law* 314.

[854] House of Lords Select Committee on Artificial Intelligence, *AI in the UK: Ready, willing and able?* (2018), available at: https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf, p. 178.

more generally (namely the European Convention on Human Rights and the EU Charter of Fundamental Rights).

1.7. In order to further enhance public trustworthiness and accountability, Human Rights Impact Assessments should be externally and independently verified by those qualified in the area of human rights law. Further technical expertise may also be required in order to confirm to the public that new AI-driven measures have been reviewed by those familiar with the relevant technology and the related risks.

1.8. This latter oversight role could be provided by the Information Commissioner's Office in line with its existing obligations under the Data Protection Bill 2017 and the explicit goal in its Technology Strategy 2018-2021 'to engage with organisations in a safe and controlled environment to understand and explore innovative technology'.[855]

2. Protecting Freedom of Expression[856]

2.1. The dangers of censorship, when internet intermediaries are used to implement government policy, are well recognised; a 'standard' application of Article 10 of the European Convention on Human Rights (ECHR) (the right to freedom of expression and information) case law may ensure the proportionality of any such State requirements, bearing in mind the risk of collateral censorship.[857]

2.2. When considering situations where an individual is blocked from a particular service, the difference between implementation of State policy and the exercise of the service provider's own rights must be recognised. Rights claims like, in general, against the State not private actors. Even here, however, the State may have obligations to take any necessary measures to safeguard a right, including enacting legislation to protect rights based on the substantive rights and Article 1 of the ECHR (the states' obligation to protect human rights).[858]

2.3. The approach to analysing whether there is a breach of rights can look different in this context - the test is one of a fair balance between the competing interests.[859] In determining whether a positive obligation exists, the Court of Human Rights has highlighted a number of factors: the kind of expression rights at stake; their capability to contribute to public debates; the nature and scope of restrictions on expression rights; the ability of alternative venues for expression; and the weight of countervailing rights of others or the public.[860] These factors would apply differently to the range of actors which are intermediaries of Internet communication.

[855] Information Commissioner's Office, *Technology Strategy 2018-2021*, available at: https://ico.org.uk/media/about-the-ico/documents/2258299/ico-technology-strategy-2018-2021.pdf, p. 8.

[856] Section author: Professor Lorna Woods.

[857] Yildirim v Turkey.

[858] Hokkanen v. Finland, 24 August 1994; López-Ostra v. Spain, 9 December 1994; Vgt Verein Gegen Tierfabriken v. Switzerland, 28 June 2001.

[859] Appleby v UK no. 44306/98, ECHR 2003-VI.

[860] Appleby, paras 42-43 and 47-49.

2.4. Overall, however, it is difficult to say that there is a user right to most of the intermediary services (because there are substitutes), especially if those intermediaries have their own freedom of expression rights which, too, must be taken into account. Positive obligations can be seen in other contexts in relation to Article 10 of the ECHR, where the State is seen as the ultimate guarantor of pluralism, and being required – in the context of broadcasting – to regulate accordingly.[861] Positive obligations also exist in relation to the State's obligation to create a favourable environment for participation in public debate by everyone, enabling them to express their opinions and ideas without fear[862], especially where there are threats of violence made against the speaker.[863] In this regard, the positive obligations upon the State may then result in regulation that limits speakers' expression in certain circumstances.

3. What information should online platforms provide to users about the use of their personal data?[864]

3.1. Importantly, platforms need to provide information as required by the General Data Protection Regulation 2016 (GDPR) and the Data Protection Bill 2017 (DP Bill). Platforms need to comply with the principles of transparency and accountability, set out in GDPR and representing crucial changes in the revised data protection regime.[865] In practice, this means that they need to explain the use of personal data in a concise, transparent, intelligible and easily accessible manner, using clear and plain language. This could be done using innovative visualisation techniques, such as layered privacy statements/notices (link to the various categories of information which must be provided to the data subject in order to avoid information fatigue), 'push' and 'pull' notices and privacy icons.[866]

3.2. As recent data scandals show (e.g. Cambridge Analytica), even providing all the information required by the data protection law is not sufficient. Platforms need to be clear as to what business model they use and what does this mean for users and their fundamental rights more generally, not only the right to private and family life. Looking beyond data protection laws, platforms also need to explain how they use user data in managing requests related to copyright infringement, defamation and the law enforcement. Some reference

[861] Centro Europa 7 v. Italy.

[862] Dink v. Turkey nos. 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09, 14 September 2010.

[863] Özgür Gündem v. Turkey no. 23144/93, ECHR 2000-III.

[864] Section author: Dr Edina Harbinja.

[865] Article 5 – 6, 12-15 GDPR, related to articles 1, 11 and 15 TFEU, see also Article 29 WP Guidelines on transparency under Regulation 2016/679, WP 260, p. 5.

[866] See Office of the Australian Information Commissioner. Consultation draft: Guide to big data and the Australian Privacy Principles, 05/2016 says: "Privacy notices have to communicate information handling practices clearly and simply, but also comprehensively and with enough specificity to be meaningful. The very technology that leads to greater collection of personal information also presents the opportunity for more dynamic, multilayered and user centric privacy notices." https://www.oaic.gov.au/engage-with-us/consultations/guide-to-bigdata-and-the-australian-privacy-principles/consultation-draft-guide-to-big-data-and-the-australian-privacyprinciples; Push notices involve the provision of "just-in-time" transparency information notices while "pull" notices facilitate access to information by methods such as permission management, transparency dashboards and "learn more" tutorials. These allow for a more user-centric transparency experience for the data subject. Article 29WP Guidelines on transparency, p. 17; similarly Information Commissioner's Office – Big data, artificial intelligence, machine learning and data protection version 2.0, 03/2017. Pp 87-88, March 2017.

to the UK law should be in place here, presented in an easily understandable language, as suggested above.

3.3. It is also important that platforms provide information regarding the use of the deceased's data and their related policies related to accounts of deceased users. Many platforms lack these policies, and many of the existing policies are not compliant with UK data protection, copyright and succession laws. Nowadays, identities are created, captured and stored online; thus, akin to testamentary freedom, users should be able to decide what happens to their data on these platforms after they die. Otherwise, we risk seeing more conflicts between platforms, friends and the deceased's family, who wish to access/delete/keep different accounts. This policy needs to be clearly presented to users on registration and later, in an intelligible and simple manner, using some of the techniques described above ('push' and 'pull' notices, privacy icons).[867]

4. The role of the UK as a global leader in Internet regulation[868]

4.1. The UK is well positioned as a global leader in many policy areas, including the Internet. Indeed, the Digital Charter affirms that 'the UK should lead the world in innovation-friendly regulation',[869] while the Internet Safety Strategy opens by asserting that 'this Government aims to establish Britain as the world's most dynamic digital economy

4.2. […by…] ensuring that Britain is the safest place in the world to be online'.[870] These sentiments are similarly reflected in the recent House of Lords Report on AI which notes that 'the UK can lead by example in the international community', and that 'there is an opportunity for the UK to shape the development and use of AI worldwide'.[871]

4.3. Yet, the Internet is a global good, and, as recognised in the Digital Charter, 'it serves humanity, spreads ideas and enhances freedom and opportunity across the world'. In this regard, as a global leader the UK holds a dual responsibility not only to deliver cutting-edge policies and approaches to Internet regulation, but also to ensure that these activities do not negatively influence or impact upon other parts of the globe. Put differently, the UK must develop broad-based policies that take into account Internet governance challenges faced elsewhere.

4.4. Indeed, one of the most critical challenges facing Internet governance in the Global South in particular, concerns the participation of such countries in the Internet governance debate. These issues of participation often reflect domestically, and can often lead to the over-regulation of the Internet by

[867] See e.g. E. Harbinja, Digital Inheritance in the United Kingdom, 21 Nov 2017, *The Journal of European Consumer and Market Law (EuCML);* Harbinja, Post-mortem Privacy 2.0: Theory, law and technology, (2017) International Review of Law, Computers & Technology. 31 (1) p. 26-42.

[868] Section author: Dr Rachel Adams.

[869] Department for Digital, Culture, Media and Sport, *Digital Charter* (2018), available at https://www.gov.uk/government/publications/digital-charter.

[870] HM Government, Internet Safety Strategy Green Paper (2017), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf.

[871] See note 3 above.

States.[872] As such, it is important to promote the work of independent national multi-stakeholder bodies in guiding Internet policy formulations and decisions, in order to support fully participatory multi-stakeholderism at a global level. The position of the African Declaration on Internet Rights and Freedoms in this regard is instructive: 'national Internet governance mechanisms should serve as a link between local concerns and regional and global governance mechanisms, including on the evolution of the Internet governance regime'.

4.5. The issue of participatory models of governance is further critical for the UK to promote in leading countries where access to the Internet and Internet resources is starkly unequal. As noted in research on the barriers facing the use of open data portals for supporting environmental governance in South Africa: 'of concern with respect to citizen open data access and use in South African are the still-low levels of broadband ICT access and, in turn, digital literacy, in impoverished South African communities […] public participatory governance processes need to take into account myriad elements of ICT availability and usage. Such elements include affordability of data, technological and data literacy, geographical locations where digital access might be difficult, and age and gender inequalities.'[873]

May 2018

[872] R. Adams, K. Yu and C. Darch, 'Taking back control through openness and inclusivity? The case of Internet Governance in South Africa' chapter in *Internet Governance in the Global South* (University of São Paulo Press, forthcoming 2018).

[873] R. Adams & F. Adeleke (2016) 'Assessing the potential role of open data in South African environmental management', *The African Journal of Information and Communication* (AJIC), 19, 79-99.

Institute of Practitioners in Advertising (IPA) – written evidence (IRN0045)

About the Institute of Practitioners in Advertising (IPA)

1. The IPA, Incorporated by Royal Charter, is widely recognised as the world's most influential professional body for practitioners in advertising, media and marketing communications. It has a well-earned reputation for thought leadership, best practice and continuous professional development and also provides core support and advisory services for its 320 corporate members who handle over 85% of advertising spend. Based in the United Kingdom for 100 years, IPA programmes can be found in more than 60 countries worldwide. Its membership is primarily made up of advertising agencies.

2. The IPA progresses media policy issues through its Media Futures' Group which meets every month and which is made up of representatives from the UK's media agencies. IPA media agencies handle the planning and buying of approximately 85% of UK display advertising spend.

3. The IPA is one of the tripartite stakeholders that make up The Advertising Association (AA) which represents advertisers, agencies and media owners.

4. The IPA also supports the points made in The Advertising Association submission on this topic, and its previous response to The Government's Digital submission (November 2017).

Why UK agencies matter

5. UK advertising, media and marketing communication agencies sit at the heart of a much larger UK creative industries ecosystem. We employ 35,000 people (27,000 of whom work in IPA member agencies). IPA member contribute approximately £66m in tax revenues. Because of the nature of our work we also directly impact other companies' growth prospects: for example, advertisers (domestic and global) and other creative businesses eg production companies.

6. The advertising industry is seen as a bellwether for the wider economy – the IPA Bellwether Report in particular is a forecasting tool that has accurately anticipated both the last downturn and upturn. It is a quarterly survey of client spending intentions. The 1Q 2018 Report (published 18th April 2018) reports that spend on internet advertising has been the strongest category over 35 consecutive quarters.

7. The Advertising Association/Warc expenditure report 4Q 2017 (published 2^{6th} April 2018) shows that the internet accounts for more than half of advertising spend (£11bn out of £22bn) and is forecast to grow another 9% in 2018.

The UK Digital Economy

8. The United Kingdom is one of the most advanced digital economies in the world. It is ranked as one of the world's digital elite in research by Mastercard and The Fletcher School at Tufts University. The UK has also been identified as one of the so-called "Stand Out" economies, characterised by high levels of digital development and a fast rate of digital evolution.

9. The UK is a global leader in ecommerce and has arguably the most advanced digital media market of any major national economy; UK digital adspend is as large as Germany, France, Italy and Spain combined.

10. We welcomed and support the Government's commitment to "create the foundations for the UK digital economy to thrive" and that "the UK should lead the world in innovation-friendly regulation".

Existing self-regulation and supporting initiatives

11. The UK's self-regulatory framework – administered by the Advertising Standards Authority (ASA) – already covers all digital advertising, including marketing. The industry is committed to maintaining an effective self-regulatory system which is a crucial element in making and keeping the UK a leader in digital advertising and serves as a blueprint for successful advertising regulation in many markets around the world.

12. The industry has developed a cross-industry self-regulatory initiative, the Display Trading Standards Group (DTSG) that is governed by the Joint Industry Committee for Web Standards in the UK and Ireland (JICWEBS). The DTSG has developed tools to provide transparency and enable buyers to actively manage campaigns and minimise the risk of ad misplacement. It has also published good practice principles for all business models involved in buying, selling and facilitating digital display advertising. There are currently over sixty signatories, covering a significant proportion of the market. JICWEBS is also working with other partners on combatting fraud eg US-based Trustworthy Accountability Group (TAG) and the City of London Police's Intellectual Property Crime Unit (PIPCU).

The IPA submission:

13. The IPA believes that the internet has proved itself to be a powerfully influential and potent business and personal tool. The unprecedented pace of its growth has meant its influence and effects on society are still not fully known or understood. It is a complex and ever-evolving channel, especially with the unchecked rise of social media. As with all things, with great power comes great responsibility.

14. Our submission will focus on commercial matters particularly with regard to the free, advertiser-funded internet. It is our view that these have a direct relationship to many of the consumer-facing matters raised by the

submission and we will attempt to provide a commercial perspective to these.

15. Our submission calls for continuing support for the industry's **self-regulatory system and its current initiatives**.

16. We have already noted, welcome and support the importance placed on self-regulation by the House of Lords' Communication Committee on "UK advertising in a digital age (published 27th March 2018)".

> *"It is in the interests of the whole industry to take greater steps to self-regulate through independent third parties such as JICWEBS. We think that the largest industry bodies should commit to signing up fully to JICWEBS. We recommend that the industry should give these bodies greater powers to create and enforce rules establishing robust industry standards on measuring effectiveness and third-party verification. If businesses fail to do so, the Government should propose legislation to regulate digital advertising."*

17. The IPA is proud to be a founding member of JICWEBS.

18. The IPA supports the same rules and self-regulations for the internet as it does for offline media: that businesses take responsibility for delivering parity of brand safe content for advertising.

19. We support self-regulation for ad-funded businesses by cross-industry bodies, eg JICWEBS, and not by individual businesses or the platforms themselves.

Political Advertising

20. Our submission also covers political advertising rules under our responsibilities as a body Incorporated by Royal Charter where we have a duty to "advance the theory and practice of advertising, media and marketing communications in all its aspects for the benefit of the public."

21. We believe the use and abuse of the internet, especially social media, are beginning to have a profound effect on political systems around the world, including western liberal democracies like the UK.

22. We are therefore taking this opportunity to reiterate the concerns and recommendations which we have already made public (April 2018).

23. We have two major concerns:

1) A successful democracy relies on its political views being aired in a public forum: "the public square". We, believe that micro-targeted political ads circumvent this because very small numbers of voters can be targeted with

specific messages that exist online only briefly and so are not available to the broader public.

2) Political advertising, unlike every other advertising category, is not covered by the Advertising Standards Authority (ASA) Codes.

24. We have therefore publicly made two recommendations for this specific form of advertising online:

1) We have called for a moratorium on micro-targeted political advertising online until we can agree a minimum limit for numbers of voters sent individual political messages.

2) We have called for a public register for political advertising. This register would require all political advertising creative work to be listed for public display so that messaging, for as long as it is not regulated, is transparent and accountable, and available to all members of the public to see should they wish.

25. On 21.1) and 21.2) the Committee is respectfully advised that we have already written to The Electoral Commission and the Party Chairmen of the main political parties to begin exploratory discussions. We very much hope to be in a position to furnish The Committee with further views when we are invited to give oral evidence.

Online safety

26. Our primary focus is to ensure that brands/advertisements are only seen alongside appropriate content.

27. We believe this commercial perspective indirectly effects the online safety of individuals because platforms are required to filter content and avoid the monetisation of inappropriate content in order to provide the necessary reassurances to advertisers/brands. We believe there is little commercial motivation to host content that cannot be monetised.

28. We therefore conclude that because of their digital advertising spend, advertisers/brands, with their advertising agencies, are already a significant influence on content without preventing any form of freedom of expression and information.

29. We have welcomed the recent initiatives by Google Youtube on this topic, which includes their recent commitment to JICWEBS' Digital Trading Standards Group certification. However it is worth the Committee noting that Google are not following up on some of the recommendations, notably around switching off comments by default on children's videos and news; and more protection around automatic upload for content, which includes children.

30. We have noted and welcomed Facebook's commitment to sign up to JICWEBS DTSG certification by the end of July, 2018.

Personal Data/Privacy

31. We respectfully suggest that the House of Lords Select Committee on Communications consider the impacts of GDPR in due course after its 25th May 2018 deadline.

Conclusion

32. We are calling for continuing support of the existing self-regulatory system through the ASA and JICWEBS's initiatives, and are making two recommendations on political advertising rules (see 21)

Specific Questions and Answers

1. Is there a need to introduce specific regulation for the internet?
We agree with the House of Lords Select Committee on Communications that the default approach to digital advertising should be self-regulation. We further note this requires online businesses and associations to fully sign-up to cross-industry bodies such as JICWEBS.

2. What should the legal liability of online platforms be for the content they host?
Legal liability as a whole is outside of our purview, however, we believe online platforms' responsibilities to provide content suitable for advertisers and the public are in parity to offline media businesses.

3. How effective, fair and transparent are online platforms in moderating content they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?
Our focus is on the moderation of content that is made available to advertising. YouTube have and Facebook will (as of July 2018) be certified within industry self-regulation structures in this space. We have expressed concerns to the platforms about moderation of comments sections, Our suggestions have not (as at submission date) been acted upon.

4. What role should users play in establishing and maintaining online community standards for content and behaviour?
Users alone cannot be relied about to maintain community standards for content and behaviour. Independent self regulation above-and-beyond this is required.

5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

Our focus as a professional industry body is on online brand safety whereby advertising messages do not run in the context of content the advertiser and indeed society at large consider inappropriate.
This plays indirectly into the online safety of individuals. Platforms must filter content and avoid monetisation of inappropriate content to provide assurances to advertisers. There is little commercial motivation to host content that cannot be monetised. Advertisers and their agencies help moderate content with their advertising spend without preventing any form of freedom of expression or information.

6. What information should online platforms provide to users about the use of their personal data?
   We respectfully suggest that the House of Lords Select Committee consider the impacts of GDPR in due course after its 25th May 2018 deadline.

11 May 2018

Institute for Public Policy Research, Centre for Policy Studies and Centre for the Analysis of Social Media at Demos – oral evidence (QQ 52-57)

Transcript to be found under Centre for Policy Studies

Internet Commission – written evidence (IRN0004)

About the Internet Commission

1. The Internet Commission is a new, independent initiative for a more transparent and accountable Internet. It aims to establish a new multi-stakeholder process to help reverse today's negative spiral of the unintended consequences of digitalisation, ad hoc regulation and loss of public confidence in technology.

2. We believe that transparency can be a catalyst for improvement in digital responsibility[874] practice. With the engagement of industry, civil society, policymakers and regulators, best practices can be developed and voluntary action by firms maximised.

3. We are developing a transparency reporting framework focused on how online content, including user generated content, is managed. It aims to gather evidence about how complaints are received, what action is taken and the effectiveness of that action.

Transparency as a catalyst for change

4. Procedural accountability and a focus on supporting and encouraging ethical business practice[875] can improve the digital responsibility performance of online firms.

5. Transparency has already been an effective driver of change, for example in the reduction of greenhouse gas emissions and in tackling the gender pay gap.

6. In the same way, online platforms should account for their work to tackle online harms whilst also supporting freedom of information and expression. A framework for disclosures should be developed by industry in collaboration with their stakeholders, and reports should be independently assessed and assured.

7. Disclosure, assessment and assurance requirements should be proportionate and should support innovation that is beneficial to society.

8. Increased transparency about the practices of online firms will help to identify the limits of voluntary action, so defining much more precisely the areas in which new, specific regulations may be required.

Regulating the Internet

[874] Corporate social responsibility as voluntary action to address social impact and ethical challenges of digitalization and digital services. See for example Thierry Driesens, "The rise of corporate digital responsibility", in I – Global Intelligence for the CIO, October 2017. http://bit.ly/2I1JLxw

[875] Following Christopher Hodges, "Ethical Business Regulation: Understanding the Evidence", Department for Business Innovation & Skills, February 2016. http://bit.ly/2DKUPgY

9. In the UK alone, there are at least 12 separate bodies that share responsibility for regulating Internet content and online interaction[876].

10. Given the complexity of the issues and the pace of technological change, regulation must become more agile and regulators must collaborate more with one another and with the firms they regulate.

11. Online platforms themselves are best placed to establish effective processes to ensure the safety and wellbeing of their users as well as protecting people's rights to freedom of expression and freedom of information. They must demonstrate that they do this, to the satisfaction of regulators as well as employees, customers, suppliers and other stakeholders.

12. It has been suggested that on leaving the EU, UK legislation could be introduced to shift the liability for illegal content online towards social media companies[877]. If this happens, some degree of continued protection from liability for the content they manage might be set up as an incentive for firms to successfully demonstrate fair and ethical business behaviour.

Next steps – piloting a transparency reporting framework

13. We are developing a pilot transparency reporting framework to assess how content is managed by online platforms. It includes quantitative questions about content reporting and moderation, and qualitative questions about human and automated content management and moderation processes.

14. Disclosure using this framework will enable an independent assessment of the effectiveness of content management by online platforms.

15. Arrangements are being made to establish strong, independent governance and oversight so that the Internet Commission can offer this independent assessment and assurance.

16. This framework should eventually be extended to cover the wide range of digital responsibility issues for which firms should be accountable to their shareholders and the public.

Advisory Board

Professor Erkko Autio Chair in Technology Venturing and Entrepreneurship

[876] Ofcom, Information Commissioner's Office, Phone-paid Services Authority, Internet Watch Foundation, Advertising Standards Authority, British Board of Film Classification, Competition and Markets Authority, Direct Marketing Association, Gambling Commission, Financial Conduct Authority, Prudential Regulation Authority, Independent Press Standards Organisation…

[877] "Intimidation in Public Life: A Review by the Committee on Standards in Public Life", December 2017, p14. http://bit.ly/2GGuCEU

	at Imperial College London Business School.
Professor Charlie Beckett	Director, Truth, Trust and Technology Commission at the London School of Economics and Political Science.
Bojana Bellamy	President, Centre for Information Policy Leadership, Hunton Andrews Kurth LLP.
John Carr OBE	Secretary of Children's Charities' Coalition on Internet Safety, advisor to UN, EU, ECPAT International and eNACSO.
Paul Dickinson	Shareholder activist, Executive Chair of CDP and Trustee of ShareAction.
Claire Milne	Consumer champion and independent technology consultant.
Dr Victoria Nash	Deputy Director, Policy and Research Fellow, Oxford Internet Institute.
Rachel Neaman	CEO of the Corsham Institute.
Stephen Pattison	VP Public Affairs at ARM, Chair of BCS Society Board.

24 April 2018

Internet Service Providers’ Association (ISPA UK) – written evidence (IRN0108)

1. About ISPA

ISPA is the trade association for providers of internet services in the UK. ISPA has over 200 members, 90% of which are SMEs as well as large multinational companies. We are proud to be an organisation which covers the whole Internet value chain, including companies that provide access, hosting and other online services. We represent communications providers that serve consumers and business, those that build their own networks and those that resell services.

2. Introduction

ISPA welcomes the House of Lords Communication Committee inquiry into internet regulation. The call for evidence raises a number of important issues that affects the UK public but also the conduct of online companies. These issues require careful consideration and for that reason we feel that it is important that the inquiry is conducted on the best evidence base possible.

It is important to recognise as starting point that, rather than being a ‘wild west’ as is sometimes described, the internet is already subject to both general and specific regulation and we would therefore encourage the Committee to focus its intention on how (rather than whether) the internet should be regulated. This includes oversight in various forms from a large number of regulatory or co-regulatory bodies, from the ICO, Ofcom and BBFC. Moreover, the internet is based on a complex and interlinked value chain that involves both users and a variety of online services that perform different functions. It is important to understand the individual elements of the value chain and the role and responsibilities each part may perform.

The definitions included in E-Commerce Directive provide helpful framework for the role and obligations of Internet companies:

Hosting providers: store data which is selected and uploaded by the users of their service. This data is intended to be stored for an unlimited period of time. Hosting providers can be exempt from liability under EU law if they are “not aware of facts or circumstances from which the illegal activity or information is apparent” or they “do not have actual knowledge of illegal activity or information”. Hosting providers must expeditiously remove such information once they have been made aware of its illegality.

Mere Conduits: deliver either network access services or network transmission services. They transmit large amounts of data for their subscribers. Mere conduits have liability exemptions under EU law when they are passively involved in the transmission of data. An ISP is commonly described as a mere conduit.

Caching providers: temporarily and automatically store data. Caching providers can be exempt from liability under EU law if they meet certain conditions pertaining to their storage of data.

3. How should the internet be regulated?

(Q1) Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

The internet is a heterogeneous entity that has developed organically over the last three decades and is subject to regulation and specific regulatory activity. Due to the rapidly evolving nature of the internet, self-regulation has also acted as an important part of the regulatory landscape; helping to put in place rules and procedures more quickly and effectively than formal regulation. We can see evidence of effective internet regulation already being carried out by a number of public and private bodies as well as legislation; for example:

- **E-Commerce Directive**, which sets out harmonised rules for online businesses.

- **Internet Watch Foundation (IWF)**, a self-regulatory body founded by the Internet industry that tackles online child sexual abuse content.

- **Counter-Terrorism Internet Referral Unit (CTIRU)**: This organisation is run by the Metropolitan Police and, as of December 2017, has been linked to the removal of approximately 300,000 pieces of 'illegal terrorist material' from the internet.

- **Defamation Act**, which created additional defences to tackle 'libel tourism' and new defences for online publishers.

It is also worth noting that ISPs have stronger data protection requirements than many offline providers, as set out in the Privacy and Electronic Communications Regulations (PECR). Given this, it would be inaccurate to characterise the internet as having consistently weaker protections for individuals and organisations than the offline world. An individual is more likely to leave a trace of their activity online than they are offline; for example, someone is more likely to be challenged over a post they have made on social media than a conversation they have had in the street.

The organic nature in which regulation has developed has led, in some circumstances, to variation in consistency and harmonisation; however, it has broadly worked well, establishing a balance between innovation and rights of redress. Furthermore, it has allowed for the development of the UK's digital economy, to the point where we are a world leader in terms of innovation and the digital economy. The regulation of the internet is a highly dynamic area, shaped constantly by user expectations as well as by policymakers and the industry itself.

ISPA believes that a combination of legislation and self-regulation is most appropriate for the future regulation of the internet. ISPA would also suggest that any regulatory intervention should adhere to the following principles:

- There should be a presumption in favour of the regulation of people by laws of general application.

- Regulation should ensure that offline and online conduct is regulated in an equivalent manner: what is illegal offline should be illegal online. Legality should be applied to the same degree online and offline and nothing that is legal offline should be considered illegal online.

- Regulation should be targeted at the most appropriate part of the internet value chain.
- Regulation should balance the rights of providers and users (while recognising that more than one provider and more than one user can be involved in single online interactions).

4. The E-Commerce Directive

(Q2) What should the legal liability of online platforms be for the content that they host?

(Q9) What effect will the UK leaving the EU have on the regulation of the internet?

Since its inception in 2000, the E-Commerce Directive has served both the public and the industry well with a robust and flexible legal framework. There is currently a live debate about what the nature of the regulation of the internet should be following Brexit and ISPA is eager to make constructive contributions to this debate wherever possible; however, we would caution against diverging significantly from the guiding principles of the Directive which have struck an appropriate balance between the competing considerations at play.

The 'mere conduit' definition in the Directive provides important protections for internet access providers so that they are not inadvertently brought into the scope of legislation targeted at hosting providers. The hosting protections in the Ecommerce Directive provide important safeguards for hosting providers that host the content of third parties. Furthermore, Article 15 of the Directive states that EU Member States cannot impose a general monitoring obligation for internet intermediaries. This means that intermediaries do not have to monitor the information which they transmit or store, nor actively seek indications of illegal activity being undertaken. In order to safeguard both ISPs and user rights, it is important that such protections provided under the Directive are preserve and incorporated into UK domestic legislation.

ISPA would stress that, when drafting legislation that affects operators along the internet value chain, the legislator should adhere to the categories described in the E-Commerce Directive and target any intervention at the entity with the highest degree of control. There is a legitimate case to look at the management of content; however, ambiguity in terminology in this area can lead to an uncertain situation in which other parts of the internet value chain or content types can be inadvertently brought into the scope of content control regulation. The voluntary approach to tackling harmful content, for example, could be addressed through Government's Social Media Code of Practice which ISPA hopes will entail robust policies on tackling harmful content and will be implemented and enforced consistently but also transparently.

Brexit provides an opportunity to make advances in this area at a pace at which is not possible at EU-level; however, we must be careful to maintain the fundamental protections afforded to both users and service providers by the E-Commerce Directive. The Government's commitment in the Digital Charter to make the UK the safest place to be online is commendable and something that our members are keen to support; however, given the need to make the UK an attractive location to do business after Brexit, there must be consistency with existing legislation. There is a danger that, if future regulation in the UK becomes significantly more stringent than that in other jurisdictions, the UK economy will be put at a disadvantage. As such, cooperation and collaboration with international partners could prove more effective and elicit a more positive result for the UK.

5. User Rights

(Q5) What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

In recent years, online content control mechanisms have been developed which go well beyond mere removal-at-source and access blocking. However, the E-Commerce Directive does not prescribe the functioning of notice and action mechanisms. Such mechanisms are founded on proactive content monitoring and are increasingly used for both mandated and voluntary content control. Furthermore, these mechanisms often depend upon the use of automatic detection technologies, as recommended in the European Commission's guidelines on tackling illegal content online.

In this situation, intermediaries find themselves being forced to act as both 'judge' and 'jury' in implementing enforcement and adjudicating disputes. This threatens to significantly undermine the rights of not only the user posting the content but also the user who may find the content harmful and the user accessing the content who does not find the content harmful.

Alongside this trend, in recent years, we have witnessed the ascent of non-judicial authorities both in the UK and the EU. These publicly funded entities act as a proxy for court oversight; they actively search for harmful online content and notify Internet Service Providers (ISPs) of the existence of such content, before recommending 'voluntary' removal. These non-judicial authorities enjoy the status of 'trusted flaggers': entities that not only make complaints about content but also make decisions about whether those complaints are well-founded.

Trusted flagging mechanisms have been found to work well in certain unique contexts; for example, the Internet Watch Foundation (IWF) has enjoyed significant success worldwide in identifying and removing child sexual abuse content. However, the unique nature of child sexual abuse material means that there is rarely ambiguity relating to its identification and illegality. The extension of the trusted flagger mechanism beyond clearly identified and bounded forms of content is unlikely to result in the same successful outcomes; this is due to the difficulty in accurately identifying illegal content without the assistance of a judicial process. Non-judicial competent authorities cannot be expected to have the same impartiality, legal expertise and interest in balancing competing rights as judicial authorities; as such, the fact that trusted flaggers are can submit takedown requests and order the suspension of domain names poses a threat to the rights of both individuals and organisations.

ISPA maintains that intermediaries should not be asked to be judge and jury and that notices should be filed by competent authorities, ideally a court or other independent and impartial body qualified and with legitimacy to make these kinds of decisions. We recognise the difficulty in having a court-based system provide an opinion on each and every incident, but we feel that this is an area worth exploring and there may be viable options available. Furthermore, content control mechanisms should always respect due process and be backed by some form of statute, with removal-at-source as the default content control measure, with access blocking to be used as a targeted and temporary resort in certain circumstances. If trusted flagging mechanisms are used, clear standards and rules should be provided by the Government in order to avoid the infringement or rights.

6. Conclusion

ISPA welcomes the Committee's exploration of internet regulation and the acknowledgement that more can be done to ensure the internet is regulated in an effective, proportionate and transparent manner. However, as highlighted above, this is an intricate policy area in which any single change carries the potential to have a negative knock-on effect all the way down the internet value chain, and throughout the economy. Given this, ISPA would suggest that any regulation is strongly rooted in the principles and protections of the E-Commerce Directive, particularly Article 15, and must be carried out with the utmost caution and clarity. In addition to this, user rights must be safeguarded against being undermined by intrusive content monitoring obligations and the rise of intermediaries being forced to act as judge and jury; thus, bypassing due process.

18 May 2018

Internet Society UK Chapter – written evidence (IRN0076)

Contribution from Dr. Olivier Crépin-Leblond on behalf of the Internet Society UK Chapter

The Internet Society UK Chapter was invited to speak at the House of Lords Inquiry on "The Internet: to regulate or not to regulate?"[878] on Tuesday 8th May 2018. The Chapter circulated the Inquiry to its membership base, triggering a wide range of feedback. In his spoken address, Dr. Konstantinos Komaitis, Director of Policy Development for the Internet Society, addressed many of the points raised in our local Chapter's consultation. The responses included in the present document, seen below, should serve an additional input from the Internet Society UK Chapter, drawing from the input and participation of our members as well as the years of experience in Internet regulation since its founding in 1992. Such policy papers may be consulted on https://www.Internetsociety.org/resources/policybriefs/.

Overall, the Internet Society favours collaboration of all actors, to reach solutions that involve a multi-stakeholder framework. We would highly suggest reading of the Internet Society paper "Internet Governance – Why the Multi-Stakeholder Approach Works" [879].

1. Is there a need to introduce specific regulation for the Internet? Is it desirable or possible?

The "Internet" is a very broad term, when referring to "regulation". In essence, it really depends on what "layers" one means by referencing "the Internet".

When considering regulation for the Internet it is important to distinguish between 'regulating the Internet infrastructure', i.e. the underlying communications backbone that facilitates the sending and receiving of information 'packets' (colloquially referred to as 'the pipes' and the "lower layers"), vs. 'regulating services that are built on the Internet' (e.g. media and commerce platforms and services.) which constitute the higher layers.
https://en.wikipedia.org/wiki/Internet_protocol_suite

Some layers (such as layer 1 and 2 that include spectrum allocation and physical properties of connectivity) are already significantly regulated. The lower layers are indeed probably not the target of this inquiry and are covered by a list of Internet Invariants which are described in a paper by the Internet Society called "Internet Invariants"[880]. Regarding Internet infrastructure, the focus should be on *facilitation of access*, which includes regulator support for the concept of Net Neutrality[881].

[878] https://www.parliament.uk/business/committees/committees-a-z/lords-select/communications-committee/inquiries/parliament-2017/the-Internet-to-regulate-or-not-to-regulate/
[879] https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/
[880] Internet Invariants - https://www.Internetsociety.org/policybriefs/Internetinvariants
[881] https://www.gouvernement.fr/en/the-digital-bill

The focus of this inquiry is therefore about the way in which we address online responsibility for users, their safety (broadly defined) and maintain their trust in the Internet.

For services built on the Internet, e.g. platforms, the primary focus needs to be on appropriate application of existing offline regulation to online service providers. Regulation (and application of regulation) should focus on the function that is provided, not the medium through which it is delivered. Thus, a business that facilitates chauffeured private car hire services should be regulated the same way, regardless if the service is provided via an online app (e.g. Uber) or an offline phone centre (e.g. traditional 'radio car' service).

A key challenge is the international nature of seamless cross-border service delivery of many online services, which can cause confusion regarding who has jurisdiction over what? This is a fundamental issue that has been recognized and addressed in the GDPR by focusing on where impact of processing occurs, i.e. the location of the data subject. The same jurisdiction issues that GDPR is addressing for personal data also apply to questions regarding copyright enforcement, taxation, hate speech, etc. associated with online businesses.

Specific consumer protection concerns arise in dealing with unbounded "in-game" purchases. Certainly for children controls need to be in place to prevent excessive charging. Given the child is not the bill payer, it could be viewed as negligence on the part of the service provider to not provide the bill payer with the controls necessary to cap such payments, something the credit card industry could champion backed by the threat to refuse to honour payments.

The fact that online platforms are increasingly becoming the information gateway for people, especially younger generations who get much of their news from online platforms via mobile devices, raises social and political concerns similar to traditional news media. Concerns about media empires with too much dominance in newspapers or TV coverage, should equally apply to online platforms where it is now common for a single provider to dominate a service sector (Facebook for social networks, Google for search). As shown by Facebook's own study (2012 US elections impact on likelihood to cast a vote[882], they have the power to influence voting behaviour.

Social concerns also arise from the fact that the majority of online platforms are developed in the US (Silicon Valley) and therefore operate under US (Silicon Valley) oriented social values which can differ significantly from EU/UK values, as for example with attitude towards the precautionary principle for consumer products or data protection laws.

2. What should the legal liability of online platforms be for the content that they host?

Online platform should be reactive to requests from law enforcement regarding take down notices whilst being cognizant of due process that respects laws.

[882] https://theconversation.com/can-facebook-influence-an-election-result-65541

On the whole, legal liability might hinder competition, as large platforms are more likely than smaller platforms, to be able to invest in resources to (a) fight litigation, (b) develop tools and algorithms to police their platform and (c) actively employ people to police their platform. When considering that historically, innovation has been shown to be brought forward by new players, hindering the ability of new players to grow through the increased risk of legal liability might hinder innovation. Furthermore, it will serve to trigger a shift of online platform hosting providers from having their servers based in the UK to migrate them abroad to more lenient regulation regimes.

However, it is also necessary to differentiate between different types of online platforms

- Public broadcast type - like open Web sites
- Private group type - like communication services such as WhatsApp
- Centralized vs. decentralized content moderation and/or recommendation such as Wikipedia

The test for legal liability must be based on an assessment of the factual role that the platform takes, not self-assessed claims regarding business sector (e.g. Facebook statement that they as a 'technology company, not a media/advertising company, should not be the determining factor in setting the regulatory regime that is applied).

Algorithmic content moderation (e.g. setting the effective visibility of content through filtering or ranking) is an editorial engagement with content, even though it does not involve direct human intervention. The platform provider controls how the algorithm is set up, what its prioritization metrics are. Platforms that provide private (encrypted) communication between closed groups should be assessed differently from platforms that provide publicly visible content broadcasting. Encrypted private communication is more similar to telephone communication, with the platform acting as neutral carrier. Net neutrality 'carrier protection' should apply to them.

3. How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

Online platforms are notoriously unclear about their content takedown process. Information regarding content moderation policy of platforms is usually provided as part of the long and complicated Terms of Service document that users typically click through without reading. Introductory demos that interactively guide new users through the features of the platforms highlight the existence and use of means by which the user can flag inappropriate content, but it is often not clear what happens once content is flagged.

Traditionally a major focus of content moderation for platform providers has been on identifying and removing copyrighted materials. In contrast to moderating of fake or hate content, where algorithmic approaches are only recently being introduced, 'pro-active' algorithms that search through the content on the platform to find potential violations of copyrighted material have been in place for many years. Just as with proposed 'fake/hate' material detection algorithms, this copyright enforcement suffers from detection errors where non-infringing material is taken down, also known as "false positives". This often occurs for content that is allowed in the US 'fair-use' copyright exemption, such as critical commentary. The process of challenging a take-down notice can however be very intimidating since this raises the chances of leading to a legal confrontation in a (US) court. This constitutes what is known as a "chilling effect".

One improvement that might be needed is the process to reverse decisions. Platforms have been accused of providing very little opportunity for a customer services contact with a real human. This brings a lack of transparency, where end users often feel as though they are dealing with an algorithm rather than a real human being.

Content takedown processes of platforms needs to introduce more transparency and processes for independent appeal.

4. What role should users play in establishing and maintaining online community standards for content and behaviour?

On the whole, end users should be associated with content takedown standards, but there are some circumstances where this is not possible.

On closed group communication platforms it is common that users have an active role in setting and maintaining standards for content and behaviour. On large open platforms, such as Facebook and Twitter, users generally do not have the means or a sufficiently global picture of what is going on in order. Responsibility must therefore lie with the platform provider. Sub-groups within the larger platforms, e.g. sub-Reddits, Facebook groups etc., do often set their own unofficial content and behaviour standards which are moderated by the users of these groups through collective responses to and infringement of those standards.

The current approach to moderation of hate-speech and only abuse, heavily relies on reporting by the abused users to trigger an investigation by the platform to determine if the content violates the platform standards. This approach makes sense as a way to avoid undue censorship of content by automated means that are likely to produce a high number (due to large volumes even a small percentage results in a high absolute number) of false-positives (the system things it is content that violates the standards even though this is not the case) and simultaneously miss many cases of actual violations. Automated methods are still not capable of reliably identifying contextual cues that can shift the meaning of content between abusive and non-abusive.

It should be noted however that regardless of failures to distinguish context, and thus producing errors, automated content moderating of copyright infringement is used by the major platforms.

A significant problem with user initiated content moderation is the response time by the platform investigation of the flagged content. Especially in cases on online abuse, any delay in action by the platform can result in increased abuse through copy-cat behaviour.

One approach could be a shift towards a model where content that users flagged as infringing of community standards is automatic temporarily quarantined, pending investigation by the platform, and released if the investigation find that the content is does not merit removal. In this case also it is imperative that the investigation by the platform must happen quickly in order to minimize the ability of malicious actors to interfere with free communication by falsely flagging content as abusive.

5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of Information?

Online platforms should publish clear guidelines on how their process for content takedown and appeal works, indicating clearly how to appeal. Platforms should also provide clear information about why content is removed or made more/less visible to users, in light of the need to protect freedom of expression.

Currently it is not uncommon that users may find that a message they posted appears not to be seen by anyone, leading to theorizing about reason why the platform might have removed or suppressed the content. It is very difficult for people to actually know if and how their content is visible to their intended audience. The same is true for companies that sometimes find out about a change in takedown policy through a sharp drop in customer engagement.

6. What information should online platforms provide to users about the use of their personal data?

One of the main problems with online platforms arises from the centralized architecture where data from/about the user is transferred to the platform provider, resulting in a loss of control over the data by the user and a strong power imbalance in favour of platform providers. Users are often confronted with an all-or-nothing choice in which they must accept complete surrender of control over their data, even if they wish to use only certain parts of the platform services. This can result in discontent and/or suspicion by the users, who might nevertheless feel compelled to use the service due to peer-pressure (fear of missing out) or lack of alternatives (for many online services there is only a single large player in the market; closed systems make it impossible to interact with users of the platform without buying in to the platform as well). The problem is often confounded by the use of an advertising based revenue model where consumer data becomes the ‘gold’ that is mined by the platform.

For all platforms that do not require log-ins, a simple process to obtain one’s personal datafile should be established and published.

For platforms that offer a log-in and therefore private accounts, each account holder/user should be able to enter an area named “what do you know about me?” where all data held by the platform about the account holder/user is displayed. Where the datafile is very large, the end user should be able to download it to their own device. They should have access to all their data and how it is being used. The uses to which data is being put should be based on fully transparent Terms of Service (ToS) and an opt-in basis. In other words the user has the ability to select and deselect the uses to which their data is being put.

Platforms should provide a clear, easily accessible overview of the various businesses, organizations and people who have received or accessed personal data of the users. This must include information that the platform has algorithmically inferred about the users, e.g. employment status inferred from times/locations of content the user posted on the platform.

Information given to the user must be in a standardized, human and machine processable format so that third party apps can be created that help users better understand the data.

7. In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

Algorithms are often considered a confidential, proprietary business asset. It is therefore unlikely that the exact workings of an algorithm be opened and transparent. However, online platforms should be clearer about where algorithms are used.

Service ‘personalization’ is frequently used to ‘optimize’ the customer interaction, this involves filtering/recommending the products/services the customer is presented with.

It is, however, often not clear what exactly is being optimized for. Is the content on the platform being shaped to provide content that will increase customer wellbeing, or is it shaped to maximise time spent on the platform and/or number of interactions with adverts even if this is to the detriment of the user?

In order to do the personalization the platforms collect a wide variety of information about the customer, including past behaviour on the platform, location tracking, scanning of content posted by the user, tracking of over websites visited by the user via ‘cookies’ and ‘tracking pixels’. Larger platforms can do a lot more with the data than smaller platforms.

The collection, use and trade of this user data, including personal characteristics inferred from this data, has potentially far reaching consequences as most vividly shown by the recent Cambridge Analytica controversy.

Concerns regarding lack of transparency about the kind of data that is collected and the purposes for which it is used apply not just to personal data about individuals but also to data about businesses.

The European Commission is currently exploring the potential for abuse of such data about business by platforms, such as travel bookings sites and online game stores, especially in cases of vertical integration where the platform provider is also a competitor in the same market (for example, the games manufacturer Valve which is also the provider of Steam, a major game selling platform.

Data-driven algorithms are an increasingly important element in determining the customer experience when using online platforms. The algorithms filter and rank which information is presented to the user and where it is presented, which affects the likelihood that a customer will notice and interact with the data. The high volumes of data available online means these algorithms are vital for enabling users to find the relevant information, be it search results, news stories of product offers. Accountability or algorithm inferences, or lack thereof, affects the development process behind the creation of the algorithms. In the current environment where the platforms are not accountable for algorithm behaviour, there is little incentive to focus on the interpretability of algorithmic processes. Due to the large number of parameters that are used by the algorithms, even the engineers who constructed the system are often not able to explain why the algorithms made specific decisions. This is even more so in the case of adaptive systems that learn from continuously evolving example data sets, as is the case with deep-learning and similar systems. We do know however, that all data-driven systems are susceptible to bias based on factors such as the choice of training data set. Since the dominant online platforms are US based, it is likely that training data sets will contain biases that reflect US culture. As demonstrated by various cases of discriminatory behaviour of algorithmic service (e.g. gender discrimination in Google Ads for high paying jobs[883]) even supposedly neutral algorithms that are based purely on observations of Internet usage statistics are not value-neutral. Rather they tend to reinforce an existing status-quo which might not be in the interest of the values that the UK society is striving for.

8. What is the impact of the dominance of a small number of online platforms in certain online markets?

The dominance of a small number of online platforms, resulting in big data, is detrimental both to plurality of data and fair competition. Competitors struggle as their return on investment are not offset by the income generated by the data analysis that comes with big data.

Thus we are in a self-perpetuating circle where local actors are seeing their local market destroyed by massive multi-national corporations that can always undercut them with better information and considerably more firepower to promote their products.

9. What effect will the United Kingdom leaving the European Union have on the regulation of the Internet?

The UK will be able to introduce local legislation that is independent of European Union legislation. Unfortunately, it is sometimes attractive to regulate too much, or too heavily, thus curbing innovation, freedom of speech and human rights. The European Union has pan-European institutions that might mitigate legislation, such as the European Court of Human Rights. The UK should continue to be a member of such organisations, wherever possible, as they are a back-stop to a healthy democracy.

International coordinated regulation is required in order to have impact, specifically on large corporations which have emerged within the US's specific regulatory framework. In this regard the EU has been an important player, where the UK will be a minor voice unless it continues to coordinate and support EU action in this area.

In data protection the status of the UK as a non-member 'third-party' participant in the EU's Digital Single Market will have implications for UK digital economy, as free flow of data between the UK and the European Single Market will be impacted.

11 May 2018

[883] https://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html

Internet Society, Julian Coles and Doteveryone – oral evidence (QQ 28-34)

Transcript to be found under Julian Coles

Internet Watch Foundation (IWF) – written evidence (IRN0034)

1. About the IWF:

1.1. The Internet Watch Foundation was founded in 1996 as a result of the Metropolitan Police notifying the Internet Service Providers Association (ISPA) that some newsgroup content being carried by Internet Service Providers (ISPs) were indecent images of children. The police believed that this may have constituted a publication offence under the Children Act (1978) of England and Wales, by the ISPs.

1.2 Following discussions with the then Department of Trade and Industry (DTI), the Home Office and the Metropolitan Police, some ISPs and the Safety Net Foundation (formed by the Dawe Charitable trust) an R3 Safety Net Agreement regarding rating, reporting and responsibility was created by ISPA, the London Internet Exchange (LINX) and the Safety Net Foundation. A key outcome of this agreement was the formation of the Internet Watch Foundation (IWF).

1.3 The IWF was established to fulfil an independent role in receiving, assessing and tracing public complaints about child sexual abuse content on the internet and to support the development of website rating systems.

1.4 Since our inception in 1996, we have operated a "hotline" function for the public to report potentially criminal content and we have been issuing "take-down notices" to UK ISPs in partnership with the Police so that they can have this content removed.

1.5 When the IWF formed, we had five funding members and our organisation has grown significantly over the past two decades. We now have 136 funding members, the most we have ever had, and employ 38 people with just over half of them analysing content we receive from public reports and proactive searching.

1.6 We receive 10-15% of our funding directly from the European Union and its Safer Internet Programme. We are one of the three charitable partners which make up the UK Safer Internet Centre. Our EU funding equates to 50% of our analyst salaries and we are currently having to consider future arrangements for funding after our current funding arrangement ceases post Brexit.

1.7 We currently receive no financial support from UK Government.

2. Scale of the challenge:

2.1 When the IWF was formed in 1996, the UK was responsible for hosting 18% of the world's Child Sexual Abuse Material (CSAM). Our latest annual report figures (2017) show that hosting of this content in the UK remains under 1%. The success in reducing UK hosting of CSAM is as a direct result of our self-regulatory model and partnership approach with the internet industry, law enforcement and Government.

2.2 In the last three years we have seen a growth in content being hosted in Europe, particularly in the Netherlands. Three years ago (2014) 57% of the worlds CSAM was hosted in North America and 41% in Europe. Today (2017), Europe hosts 65% of the world's CSAM and North America 32%.

2.2 In 2017, our analysts processed 132,636 reports of suspected child sexual abuse. Of these, 80,318 (61%) were confirmed as CSAM. Of those reports, 50% came from the public and 50% were proactively sourced by our analysts. 43% of children appearing in these reports were between the ages of 11 and 15 and 86% were girls. We also found that the younger the victim, the higher the level of abuse they suffer with 63% of images of abuse for the age range 0-2 being classified as Category A (the highest level of abuse).

2.3 In partnership, with the independent think-tank Demos, the IWF in January this year launched a report which highlights the scale of the challenge with dealing with this content online. In 1990, the Home Office estimated there were just 7,000 child sexual abuse images, videos and tracings in circulation and today we know that police seizures regularly involve millions of illegal images being found on an offender's computer.

2.3 Estimates to assess the problem range widely, the number people arrested for "obscene publications" violations increased by 134% in 2014/15 to 7,324. In total 54,000 child sexual abuse offences (contact abuse and CSAI) were recorded in the year 2015/16 according to the Office of National Statistics.

2.4 CEOP estimates that 50,000 individuals have viewed illegal CSAI online, although the NSPCC places estimates much higher at 590,000, which means there is a wide variation in determining what the scale of the challenge is and it is difficult for us to predict just how much content there is online and how many offences can be identified.

2.5 There is no doubt that the internet has been a huge force for social good. We are better connected, better informed and more entertained than ever before, but with the evolution of new technology and the benefit that this brings, there are challenges to address with the internet ecosystem and particularly the sewerage that it creates.

2.6 One of the big problems, is that the internet has significantly changed offender behaviour. The huge volume of material and the global, borderless nature of the internet have challenged the very norms that societies are founded on. For law enforcement, they rely on borders and different jurisdictions to define their operations and with so much internet enabled crime it is becoming increasingly difficult to bring offenders to justice for all sorts of crimes where the victim is in one country, the offender in another and a crime is facilitated by a website hosted in a third jurisdiction. Under which legal process do you have the trial and who is responsible for bringing someone to justice in that scenario?

3. Our experience: Working with Industry:

Our Members

amazon.com
AT&T
BT
CISCO
facebook
Google
Microsoft
sky
TalkTalk For Everyone
Telefonica
Virgin media
vodafone
Citrix ByteMobile
McAfee
paloalto
Symantec.
TATA COMMUNICATIONS
THE UK CARDS ASSOCIATION
Oath: YAHOO!
Check Point
FORTINET
GIGANEWS
3
linx
PayPal
WESTERN UNION WU
BAE SYSTEMS
Barracuda
FORCEPOINT
SOPHOS
FOR ALL
Trustwave
WEBROOT
Adobe
Allot communications
BlackBerry
SANDVINE
The Walt Disney Company UK & Ireland
WatchGuard
zscaler
adaptivemobile
Akamai
badoo
BBC
crisp
CYREN
Dropbox
exa networks
G2 Web Services
iboss NETWORK SECURITY
impero
JAGEX
Jisc
KCOM
Lightspeed Systems
LONDON GRID FOR LEARNING
NetSupport
netsweeper
NOMINET
Omicron
Openwave Mobility
POST OFFICE
RM Education
Royal Mail
NetClean
schools BROADBAND
securly://
smoothwall
SONICWALL
sure
TESCO mobile
WEBSHIELD
zen
zvelo We categorize the Web
Afilias
askfm
CHAINALYSIS
donuts
ELLIPTIC
GSMA
ICM REGISTRY
ISPAUK
JT
names.co.uk
iomartcloud
SAFEDNS
Sheffield Hallam University
TELEHOUSE
UseNeXT
webs
YH GfL
BLOCKCHAIN INTELLIGENCE GROUP
CITHREE
LONDON
E2BN
futuredigital
icuc•social creating common ground
IT Systems
netopian
NOTTINGHAM TRENT UNIVERSITY
OneTek BUSINESS SOLUTIONS
QUICKLINE
SAFETONET
Securus
seethelight
usenet.nl
avanti
BRIGHTSTAR
BYPASS
Diladele B.V.
DNSFilter
evolveODM
HUSHKEYS
OAKFORD
Opendium e-Safety
plan.com
rawstream
senso
The Social Element
XS NEWS
yubo
EE
Rightside
tumblr.
Relish

3.1 The IWF has over twenty years of dealing with these issues and has developed a strong working relationship with the internet industry, law enforcement and Government, both in the EU and UK of effectively dealing with the spread of child sexual abuse material online.

3.2 We believe that our model of self-regulation has been particularly effective, because at a time where the political environment has been uncertain, dominated by issues such as the 2008 financial crisis, fixing the economy and Brexit, these issues have not affected our collaborative approach with the internet industry. Our industry members fund our work and when they sign up to the IWF we ask that they do all that they can to stop the spread of this illegal material online.

3.3 Many of our big fee-paying members go above and beyond just paying the IWF membership. Google for example gave us £250,000 per year for four years to expand our team of Internet Content Analysts by seven people. Facebook and Twitter regularly pay for our staff to attend their internet safety events, with our Deputy CEO recently attending an event in Dublin and our Hotline Manage due to attend and event in San Francisco this summer.

3.4 They also lend us technical expertise as well as financial support. Microsoft, Cisco and Google have all sent us engineers to spend a week with us.

3.5 We have also worked directly with the industry to develop products and services to directly stop the spread of Child Sexual Abuse Material online. Our founder member BT worked closely with us to develop a URL blocking list as part of their “cleanfeed” innovation, which currently has on average 6,000 illegal URLs containing child sexual abuse on it and is reviewed daily by our analysts.

3.6 Microsoft developed PhotoDNA which enables them and us to create a unique Hash, (a unique fingerprint formed by a series of unique letters and numbers for each image), which then prevents this image being reuploaded to the internet once it has been defined as illegal. As the majority of images, we deal with are duplicates, this helps prevent revictimisation of children in the images and also prevents ordinary members of the public stumbling across this content online. We are now working closely with them to develop PhotoDNA for Video which will enable us to act on specific video clips that we know contain child sexual abuse. At the time of writing this submission, we have over 300,000 unique illegal images of child sexual abuse on our Image Hash list. This is deployed daily by a number of major companies including Facebook and Google to stop the uploading of any duplicates on their platforms and is also used by the IWF in our proactive programme.

3.7 Over the past three years, Microsoft has also provided £15,000 annually in research grants to the IWF and this has enabled us to be an authoritative voice on the current trends, patterns and research in this area, with the latest piece of research based called "Trends in Online Sexual Exploitation: Examining the Distribution of Captured Live Streamed Child Sexual Abuse" due to be released in May 2018.

4. Our experience: Working with Government and the need for legal certainty

4.1 Whilst we clearly gain a lot of expertise, support and assistance from the internet industry, it is important to recognise the role that Government plays in our partnership approach to dealing with this content. We work closely with a number of Government Departments including the Home Office, Department of Digital, Culture, Media and Sport, Cabinet Office and Number 10 Downing Street in order to play our part in making the UK "the safest place to go online." We also work with Parliamentarians in Westminster, the European Parliament in Brussels and in the devolved administrations as we also recognise the importance of advocating our work at a local level. We currently have 75 political champions a number of w whom hold senior Cabinet and Shadow Cabinet positions.

4.2 One of the many lessons we have learned over our twenty plus-years of operation is that there is a need for legal certainty when removing content online and Government and politicians have a crucial role to play in defining what is and isn't illegal.

4.3 For Child Sexual Abuse Material, there is a clear legal framework, which is broadly accepted globally which has made it possible for us to be so effective at what we do.

4.4 In the UK, the Protection of Children Act (1978) makes it an offence to take, make, possess, show, distribute or advertise indecent images of children. The Criminal Justice and Immigration Act (2008) went further and built upon the Protection of Children Act, by extending the definition of a photograph to include tracings, derivatives and pseudo images whether made by electronic or other means and the Coroners and Justice Act (2009), went even further by defining Non-Photographic Images of children (manga and hentai for example) and made these illegal in the UK, the only country in the world to do so.

4.5 The IWFs remit is based on these laws, to remove Child Sexual Abuse Imagery wherever it occurs and to remove Non-Photographic Imagery (NPI) Child Sexual Abuse Imagery hosted in the UK.

4.6 We can assess content severity levels due to guidelines produced by the Sentencing Council. Their 2014 guidelines, mean that our analysts can define illegal child sexual abuse material following a three-step categorisation process as set out below, these are the same guidelines used by law enforcement and the judiciary use in bringing offenders to justice:

Category	Description
A	Image involves sexual penetrative activity; images involve sexual activity with an animal or sadism
B	Images involve sexual, non-penetrative sexual activity
C	Other indecent images not falling under Category A or B
Not illegal	The image is not deemed to be illegal.

4.7 It is important to recognise that the IWF also has no powers by statute. Our operations are governed by a Memorandum of Understanding between the National Police Chiefs' Council (NPCC), the Crown Prosecution Service (CPS) and the IWF and is linked to Section 46 of the 2003 Sexual Offences Act.

4.8 The industry is responsible for acting on illegal content online because of the Directive 2000/31/EC of the European Parliament and Council of 8th June 2000 on certain legal aspects of information society services electronic commerce, in the internal market ('Directive on Electronic Commerce').

4.9 The E-Commerce directive under section 40, creates "a duty to act, under certain circumstances, with a view to stopping or preventing illegal activities" it continues: "this directive should constitute the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information; such mechanisms could be developed on the basis of voluntary agreements between all parties concerned and should be encouraged by Member States."

4.10 For the IWF this enables us to issue "Notice and Take Down" reports to the UK Internet Industry once our analysts have assessed an image as being illegal.

4.11 We have some of the fastest removal times anywhere in the world and our latest Annual Report statistics show that 53% of content was removed within two hours of a notice and takedown being issued.

4.12 Sections 17, 18 and 19 of the E-Commerce Directive relates to mere-conduits, caching and hosting are also of relevance to the IWFs activities and are essential to our collaborative approach with the internet industry. We would be keen to see these sections retained in their current state, if the Government considers reforming the Directive (particularly once Britain leaves the European Union) as has been hinted and recommended recently by Lord Bew's Intimidation in Public Life: A review by the Committee of Standards in Public Life.

4.13 It is our belief that content that is deemed to be harmful and which should be removed from the internet should be defined in law and not subject to discretionary, subjective interpretation. We strongly believe, based on our experience, that this process should be independent of Government and free from political interference.

4.14 We also believe that the process for removing content from companies should also be independent of individual companies themselves. If left to individual companies, commercial imperatives can too easily shape decisions, and, in any case, smaller companies cannot afford the reviewing mechanisms that larger companies can. There is a myth that the tech industry is a-wash with money and the brightest and the best brains, with the ability to solve all the world's problems and whilst that may be true of some of the larger players, there is a need to recognise that much of the tech industry in the UK is made up of small start-ups that do not have access to the sorts of resources Government think they do.

4.15 It is our opinion that an independent process with company membership needs to be established, governed by a majority of independent board members, drawn from relevant stakeholders on the particular type of content that is being regulated.

5. Our Experience: Working with Law Enforcement:

5.1 The IWF has worked closely with law enforcement ever since its inception in 1996. Whilst we do not get involved in the investigative process, we complement law enforcement by offering a secure and anonymous place for the public to report and are currently one of the only hotlines in the world permitted to proactively search for this material online. In the UK, we work closely with National Crime Agency (NCA) Child Exploitation Online Protection (CEOP) team and our CEO sits on their Command Strategic Governance Group. Our Deputy CEO is a member of their Command Prevent Board. We also work closely with the Government (Home Office, RICU Team) in running an educational awareness programme that target 18-24-year old men who we know are most likely to stumble across this content online, to know the law and how to report if they do stumble across CSAM online.

5.2 We work closely with NCA CEOP and our CEO sits on their Command Strategic Governance Group and our Deputy CEO is a member of their Command Prevent Board.

5.2 What is clear to us is that the volume of material being unearthed by ourselves and law enforcement is presenting significant challenges to them. The IWF has graded 500,000 images for law enforcement to assist their development of the Child Abuse Image Database (CAID) and we are the first non-law enforcement agency to have access to this database, further highlighting our trusted position with Government and Law Enforcement, but much more needs to be done.

5.3 We would like to be able to use CAID data to supply hashes to the UK based internet industry in the form of hashes to ensure that even more illegal images than just the IWF data sets are able to be given to industry to prevent them being reuploaded to the internet and further reducing revictimisation. We have already piloted this approach with six companies with the agreement of the Home Office and are currently in discussions with the Department about how this can be further expanded.

5.4 We also believe that if we are going to ever come close to eradicating the spread of child sexual abuse imagery on line then this requires law enforcement to be properly resourced, both financially, technically and have people with the right skills in order to respond to highly sophisticated methods used by offenders producing and consuming this material. Issues such as end to end encryption, live streaming of abuse and expansion in the use of "hidden services" (websites hosted within proxy servers- otherwise known as the dark web), makes it almost impossible for law enforcement to produce an evidence trail for as it leaves little or no digital footprint for law enforcement to investigate or use as evidence in court.

6. Specific Questions posed by the inquiry:

6.1 Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

6.1.1 We believe that the IWF's model works because there is a legal framework in place which defines what is illegal and what isn't illegal. This means that there is a clear standard for the IWF to enforce against in respect of Child Sexual Abuse Material (CSAM) online. There is also a legal framework in place which means that providers are liable for the content that they host through the e-commerce directive, which requires them to take action against illegal content once it is made aware to them and we believe that our model could be an example that could be replicated for other forms of internet harms.

6.1.2 We believe that the IWF model of self-regulation is unique and works, evidence by our impact over the last twenty-years and shows what can be achieved when there is legal certainty, an independent assessment process, transparency over what has been removed and a rigorous review process to ensure accountability over the decisions made.

6.1.3 It is our view that self-regulation does work where there is legal certainty over what is and isn't illegal. We do appreciate, however, that even though laws can define a legal framework, there are other challenges to overcome such as freedom of expression, which can be hugely subjective, difficult to define in law and technically difficult to enforce against.

6.1.4 The global, borderless nature of the internet does present unique challenges and cultural differences across different jurisdictions, which does make internet regulation particularly challenging where there is not international consensus on what is defined as illegal content.

6.1.5 Our work in removing CSAM online, however, is globally renowned, respected and experiences good levels of co-operation. Internationally, we play an active part in the WEPROTECT Global Alliance with our CEO sitting on its International Advisory Board and the UN's International Telecommunications Union (ITU) Child Online Protection (COP) Steering Group. We work closely with Europol and Interpol and by actively participating in Europol's EC3 meetings, related to European Cybercrime.

6.1.6 As a founding member of the INHOPE Association of hotlines (51 hotlines in 45 countries), we work with other hotlines to remove content hosted in other countries where a hotline exists. In the absence of a hotline in a country found to be hosting content, thanks to the legal support provided by law enforcement and a global acceptance of CSAM as being illegal, we can speed up the removal process for this content by working directly with law enforcement in a country where a hotline does not exist.

6.1.7 We are also currently implementing a three-year programme, funded by the Global Fund to End Violence against Children to establish 30 international reporting portals in the most underdeveloped countries in the world, to ensure that they have a place to report as internet penetration in those countries continues to grow. We currently have 13 reporting portals in British Overseas Territories and 8 other portals established in India, Belize, Namibia, Uganda, Tanzania, Mozambique, Mauritius and Malawi.

6.1.8 There are currently no bright ideas of how to introduce effective internet regulation without damaging the delicate infrastructure and eco-system which has made the internet such a valuable tool in the first place. Internet companies also do not see regulations as a credible threat as legislators often lack the technical "literacy" to understand what can be achieved in engineering terms, and, in turn what the useful role for regulation might be. Given the critical importance of internet based services and products to the UK economy the danger of unintended consequences particularly to smaller firms or start-ups (vital to the UK economy), of poor legislation needs to be very carefully considered.

6.2 What should the legal liability of online platforms be for the content that they host?

6.2.1 The IWF's model is based on trust and confidence of the internet industry in the assessment that is made by our analysts. In a time of political uncertainty, the IWF has made great strides forward in tackling illegal child sexual abuse material online, under the current regulations.

6.2.2 The e-commerce directive as outlined under the section which calls for legal certainty is particularly important to the IWF's activities and function. Without making platforms liable for the content that they host, it would be very difficult for the IWF to enforce "notice and take down" procedures, block access to illegal content and ultimately remove this from the internet, which will create more work for an already stretched law enforcement in the longer term. Any changes to this directive will create uncertainty and could have an impact on the spread of child sexual abuse material online.

6.2.3 We believe that the current legal framework for liability already exists and does not require any further changes of amendments for companies to cooperate with the removal of illegal content online.

6.3 How effective, fair and transparent are online platforms in moderating the content that they host? What process should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for reviewing this?

6.3.1 There is no doubt that online platforms need to be much more transparent in how much content that they are removing from their platforms. However, we also believe that any independent bodies that are also recommending to platforms content that should be removed are equally as transparent.

6.3.2 We support proposals contained within the Government's recent Internet Safety Strategy to introduce a transparency report and a voluntary code of practice which ensures that companies maintain processes and deal with notifications swiftly and efficiently and give clear explanations to the public about action taken against content. We believe that this approach should be voluntary, rather than statutory, as there have already been efforts by companies such as Google, to be much more transparent in the amount of content that they remove online and with both Facebook and Google announcing that they are making significant investment in personnel and technology to focus specifically on this. It is also clear, from our experiences that self-regulation can work, if the Government is clear on expectations of companies, but should not underestimate the complexities of the challenge as set out in the introduction to this response.

6.3.3 The IWF believes that users should have the right to appeal the legality of content that is removed from the internet, but that this should be a part of a range of measures to ensure compliance with the law. There have been examples of internet users reporting content to companies of information that is true but embarrassing in the way that wealthy and powerful people use UK defamation laws to protect their interests. We believe that companies and bodies responsible for the removal of content should ensure that those responsible for making decisions about the removal of content are trained to a high standard and supported both psychologically and managerially. We also believe that their decisions should be quality assured through a rigorous internal process and externally audited. Ultimately, any challenge to the legality of content should be subject to judicial review.

6.3.4 The IWF would be happy to co-host a series of roundtable events which debate and consider the right response to the form of content being regulated, based on our extensive knowledge and experience of working with industry, law enforcement and Government.

6.3.5 At the IWF, we gradually expose our analysts to the types of content that they will be reviewing and it can take six months to properly induct them before they are fully exposed to the most severe forms of content.

6.3.6 We ensure that they have mandatory counselling monthly, and are subject to a mandatory psychological assessment with an experienced professional to ensure that they are still able to cope with the process. We also ensure that for certain tasks such as hashing that regular breaks are taken to ensure that we are looking after their welfare effectively.

6.4 What role should users play in establishing and maintaining online community standards for behaviour?

6.4.1 The IWF is one of three charities (including SWGfL and Childnet International) who make up the UK Safer Internet Centre. There is a wealth of resources on the UK Safer Internet Centre webpage which provides advice and support to children, their parents and those professionals working with children and young people.

6.4.2 For children there are interactive games and quizzes, films and advice about staying safe online, with latest blog postings giving advice on how to spot advertising on Instagram and how to control your privacy settings on the platform.

6.4.3 For Parents, there is advice about safety tools on social media networks and other platforms, a parent's guide to technology and advice about how to have a conversation with your child about safe internet usage.

6.4.4 The website also provides Teachers with teaching resources, curriculum planning and appropriate filtering and monitoring.

6.4.5 All three charities that make up UKSIC believe that users play and important part in maintaining standards of behaviour online and that is why we run the UK's Safer Internet Day to encourage greater responsibility of children, parents and carers and those working with children and young people.

6.4.6 The day has been running in the UK for the last past eight years and the 2018 theme was specifically focussed on promoting more respectful behaviour online with the slogan: "Create, Connect and Share Respect a better internet starts with you." This day reached 45% of children aged 8-17 in the UK and 30% of parents and was supported by over 1700 organisations. We also believe that there is a need to educate children about the nature of the online world and how it works and operates.

6.4.7 The current political narrative in general places a lot of blame at the doors of the large tech companies for "needing to do more" to remove illegal and harmful content online. However, there are examples of flawed legislation which will have a negative impact on the availability of information, the freedom of expression online and many other of the internet's benefits if Britain decides to introduce greater regulation through proposing legislation by that focusses all their attention on "tech companies needing to do more."

6.4.8 One example of flawed legislation is the NetzDG law in Germany which requires companies to remove illegal content online or face large fines of up to 50 million euros. This is seeing companies removing more content than they should, some of it even legal, to avoid being heavily fined. Now politicians in Germany are calling on reform to the law to ensure that users also play their part in making the internet a safer place.

6.5 What measures should online platforms adopt to ensure online safety and protect the rights and freedom of expression and freedom of information online?

6.5.1 The UK Safer Internet Centre, again contains a number of resources which encourage people to express themselves online and to ensure that they do so respectfully. The UK Safer Internet Centre has produced a number of Social Media Guides relevant to all of the major platforms about online safety features and how to use their platforms responsibly.

6.5.2 The UK Safer Internet Centre, also provides a "one stop shop" to sign post those needing help to the right relevant organisations that can assist them with their specific concerns (hate speech, removal of suspected CSAM etc.) through the need help? Section of the website.

6.5.3 There are also a number of proposals contained within the Government's Internet Safety Strategy green paper, which include giving children and adults a greater understanding about their online safety. The Childnet Digital Leaders programme, supported by Facebook, puts young people at the heart of a whole schools' approach and ensures internet safety learning is fun and effective.

6.5.4 Google has an "Internet legends programme" to educate primary school children in the UK to empower children and act responsibly online. The programme was designed in partnership with Parentzone, Childnet and the Oxford Internet Institute.

6.5.5 It is initiatives like these that educate children and young people about responsibility online which play a vital role in ensuring that children are aware of what is and isn't acceptable online and the importance of their role in playing a responsible part of the internet eco-system.

6.6 What information should platforms provide to users about their personal data?

6.6.1 It is not for the IWF to comment on what platforms should provide to their users about their personal data. However, the GDPR legislation sets out provisions on informed consent that are consistent with international human rights norms.

6.7 In what ways should online platforms be more transparent about their business practice - for example their use of algorithms?

6.7.1 How public companies should be about the algorithims they use is a complex question as it goes right to the heart of the business model of the internet.

6.7.2 The sheer volumes of content now available online means that algorithms are now a vital tool used in identify harmful and illegal content online. However, if they come across potentially questionable material online, we believe that it is important that human analysts have the final say on any recommendation to have any content removed.

6.8 What is the impact of the dominance of a small number of online platforms in certain international markets?

6.8.1 Many of the smaller platforms do not have the capacity and resources to review illegal content and remove it, they are simply trying to make themselves commercially viable in the first instance. It is therefore important that all companies no matter their size can rid their platforms of illegal content online and that proposals such as designing in safety by design, proposed in the internet safety strategy are implemented.

6.8.2 The IWF operates a tiered approach to membership which sees the largest firms paying £79,000 per year for membership and the smaller platforms paying £1,060 based on the size and sector in which the firm operates. This means that we will work with all members and give them access to the services that they need in order to improve online safety for their users.

6.8.3 Clearly, the dominance of some companies does create challenges for the IWF. We have seen a number of mergers and acquisitions of companies which does have an impact on our ability to leverage more funding from the internet industry as there are less companies to contribute to membership fees if they have been brought out.

6.9 What effect will leaving the European Union have on the regulation of the Internet?

6.9.1 For the IWF there are several risks presented through Britain leaving the European Union. We will lose 10-15% of our funding as a result of no longer being eligible as a member state for funding. Our current funding period runs until December 2018 and we are currently applying for a further round of funding which should secure funding until 2021, however, after that we will have to find alternative revenue streams. This could significantly impact on our ability to remove illegal CSAM online as the funding equates to 50% of our analyst's salaries.

6.9.2 With the UK enshrining all current EU legislation into UK law, there is the potential for the UK Government to make changes to existing EU legislation. One of our big concerns is that any reform to the e-commerce directive could change the nature of our relationship with the internet industry and make enforcement of notice and take down and blocking challenging, particularly if the liability framework for companies contained within this directive is altered.

6.9.3 Our recent annual report also states that over the past three years we have seen a gradual shift in the hosting of illegal child sexual abuse material from the U.S. and Canada to Europe with now 65% of content being hosted in the EU. We are concerned that the UK is a world-leader in eradicating this imagery online and that without our active involvement in Europe this could have a significant impact on the safeguarding of children in both Europe and the UK moving forward.

6.9.4 Finally, the IWF recently supported, along with a number of other civil society organisations, an amendment to the EU Bill (Withdrawal) at Committee and Report stage in the House of Lords, which asked that the Government lay before Parliament a strategy to deal with cross-border law enforcement issues post-Brexit. Our concern is that Britain could potentially lose expertise from agencies such as Europol and Eurojust which will make pursuing cross-border crimes potentially much more problematic post-Brexit. It is also possible that it will be harder to pursue criminals across borders without UK involvement in the European Arrest Warrant for example.

11 May 2018

Internet Watch Foundation, Metropolitan Police, National Crime Agency and National Police Chief's Council – oral evidence (QQ 35-43)

Tuesday 15 May 2018

Watch the meeting

Members present: Lord Gilbert of Panteg (Chairman); Lord Allen of Kensington; Baroness Benjamin; Baroness Bertin; Baroness Bonham-Carter of Yarnbury; The Lord Bishop of Chelmsford; Viscount Colville of Culross; Lord Goodlad; Lord Gordon of Strathblane; Baroness Kidron; Baroness McIntosh of Hudnall.

Evidence Session No. 5 Heard in Public Questions 35 - 43

Examination of witnesses

Ms Susie Hargreaves OBE, Chief Executive Officer, Internet Watch Foundation; Chief Constable Stephen Kavanagh, National Police Chiefs' Council; Mr Will Kerr, Director of Vulnerabilities, National Crime Agency; Mr Donald Toon, Director of Prosperity, National Crime Agency; Detective Superintendent Phil Tomlinson, Head of National Digital Exploitation Service, Metropolitan Police.

Q35 **The Chairman**: I welcome the witnesses to our session on regulation of the internet. Our witnesses are from the Internet Watch Foundation and law enforcement agencies. The meeting will be broadcast online and a transcript will be taken.

Our inquiry is seeking to establish whether or not we need to regulate the internet further. While exploring that, we are very keen to look at the balance between further regulation and freedom of expression.

Will our witnesses briefly introduce themselves and tell us a bit about their background and the organisation they represent? Perhaps in your opening remarks you would tell us the main challenges that you face in dealing with internet crime, and whether the legal powers that you enjoy are adequate to face up to those challenges.

Ms Susie Hargreaves: Thank you for inviting me to speak. The IWF is the UK hotline for reporting and removing online child sexual abuse. We operate in a trusted triangle between law enforcement and the internet industry. It is a very delicate balance. Our plea is that our self-regulatory approach is acknowledged as working, as we believe it is the best way to remove online child sexual abuse; it is a model that is not broken and does not need fixing.

We are one of the most successful hotlines in the world, with an unrivalled track record for speed of removal of content, which in the UK is typically less than two hours. The UK has gone from hosting 18% of all child sexual abuse to less than 1%. The UK is one of the most hostile territories in the world for hosting online child sexual abuse. Ninety per cent of our funding comes from the internet industry and 10% from the EU.

To give you a sense of the scale of the problem, child sexual abuse is not something that we think will be solved. It is a war of attrition and we need to keep fighting to attack the crime. Last year, we removed 78,500 individual web pages of child sexual abuse, of which 90% were girls and 55% children under 10. We are talking a lot about babies who are raped and tortured. Over the last three years, 65% of the content we have removed of children aged nought to two was category A, which is rape and sexual torture.

As an example of what it means for survivors and victims, last year I met a very brave 18 year-old woman in the States. In the States, you can opt to be notified if anyone is caught with a series of your images. She was rescued when she was 12, after 12 years of appalling abuse. Her father received 60 years in prison. She had already received 1,500 notifications from US law enforcement of people being caught with her images. One of the images had been shared more than 70,000 times. Appallingly, when she was 13, a man came up to her in a supermarket and talked about seeing her images online. These are real abuse victims, and every time someone looks at that abuse the child is revictimised.

In relation to the challenges and the legal position, our model of self-regulation works and goes right to the heart of the questions posed by this inquiry. We believe there are lessons learned from the 22 years we have been in existence that we can share. We are dealing with the very worst of the internet, which we call the internet sewerage system. No other form of content online has been as successfully removed as child sexual abuse under the self-regulatory model we apply, because the definitions of child sexual abuse are widely accepted in the UK and internationally, and our assessment is clarified in UK law. Very importantly, unlike other internet harms, we do not have to go before a judge and jury for someone to take an opinion, and we can act quickly to have the content removed.

The challenges for us are threefold. The first challenges are technical. Technical solutions alone will not resolve the issue. It is important to work with the internet industry. Secondly, it is important to understand that there are social and educational issues about raising awareness of the crime. The third challenge is on the regulatory front. We believe we have the necessary laws and legislation in place to be able to act and that we are in a very privileged position to do so, but it is not a model that particularly works elsewhere in relation to other types of content.

To finish, I reiterate that we have a very delicate triangle of trust between law enforcement, the internet industry and ourselves, and we have a model that works exceptionally well. It’s not broke, so please don’t fix it.

Chief Constable Stephen Kavanagh: I am currently chief constable of Essex. I am also the lead for the National Police Chiefs’ Council for the digital policing portfolio. That is divided into three areas: how the public can contact policing in the digital age, moving on from the 999 system; how we can use that information more effectively to analyse, develop intelligence and investigate, which is to do with the skills of the officers involved; and how we can consistently present that data in the criminal justice system.

I have come straight from a digital policing board that I chaired this morning. Things are progressing in an encouraging way as regards police chiefs taking responsibility. I have been a police chief constable for five years. When I first became a chief constable, I was at a regional meeting where one of the chiefs said, "We don't have a digital policing problem". That was an enormous concern, because some chiefs did not even know what they did not know. There is now an ambition for us to try to make sure that we can work with other stakeholders to understand where those harms are taking place.

My experience as ex-commander of counterterrorism at Scotland Yard and deputy assistant commissioner for specialist operations is that a two-tier level of capabilities had been developing. The security services, counterterrorism teams and the National Crime Agency have developed a very high level of capability and very good relationships with some of the internet providers and other developers.

My concern was about mainstream policing. Where were local forces organising themselves? What was going to happen to a victim of abuse online, to someone who was harassed online and to the victim of fraud or anything else that was taking place? How could we ensure that policing was more consistent in the way it responded to victims? The 1950s "Dixon of Dock Green" model of policing is a bygone concept. Of course, we need bobbies in communities; that is part of what we must be, but we must also be fleet of foot and understand the legislation.

I have a slight concern. Some of the top-level crime sites are taken down quickly by providers. There is the capability to remove sites quite quickly when the need arises, but a lot of things are still going on both on the open web and on the dark web. Enabling legislation, with appropriate judicial oversight, can help us to go more quickly after the sites and to where the funding opportunities might be for criminal endeavours.

As to where the 43 chiefs are, the days of people saying that we do things 43 different ways are no longer true. We are increasingly consistent in the way we develop capabilities. There is an ambition within policing to be better, but also enough humility for us to say that there is an enormously long way to go to develop skills, and understand what you do at a burglary scene when a digital footprint is there but DNA and fingerprints are not. I am here both to explain where we are progressing well and to show humility about the ambition of mainstream policing to try to improve in this area.

The Chairman: You touched on a number of the issues that we want to explore today, and that is a very useful introduction.

Mr Will Kerr: I am director of vulnerabilities for the National Crime Agency. To give you a sense of the NCA's statutory responsibilities, by law it is responsible for leading the UK's fight against serious and organised crime. Steve touched on some of those responsibilities. Within the NCA my portfolio includes CSEA, which is child sexual exploitation and abuse; responsibility for CEOP, the Child Exploitation and Online Protection Centre; and organised immigration crime, modern slavery and human trafficking. Of relevance to your hearing today is that social media are being used to facilitate the criminal exploitation of vulnerable people in all three of those threat areas. Increasingly, social media are used to recruit and trade vulnerable people. This is now a global phenomenon; it is by no means restricted to western Europe or the United Kingdom.

I will take a slightly different approach to the CSEA thread, if I might touch on that briefly as a practical illustration. I think the system is broken and fundamentally needs to change, and there are simple things, particularly in our relationship with industry, that can happen to help protect thousands of young children across the United Kingdom today and tomorrow from the risk of child sexual exploitation and abuse.

I am happy to go into more detail later, but, briefly, the scale and nature of the CSEA threat has changed fundamentally over the course of the last five years. The scale has risen exponentially to the point where the law enforcement system is struggling to keep up with it. If we take industry referrals alone, we get most of them through a charity called NCMEC, which is the National Center for Missing and Exploited Children. It is housed in north America because that is where most of the big companies are based.

The number of referrals that the NCA has had since it was created in 2013 has risen 700%. That has stretched the capacity of the law enforcement system in the United Kingdom to keep up. The scale has fundamentally changed as well. All CSEA is serious. This is not about grading its seriousness, but we do need to grade its risk. The exponential rise in volume has masked the risk factors that have developed and evolved over the course of the last number of years. Live-streaming is an example.

The IWF published an impactful report today about live-streaming, but we are now dealing with organised crime gangs in Thailand, the Philippines and the Far East that are motivated not by sexual predilection but by the need to make money. A number of organised crime gangs in those countries are now engaged in the live-streaming of content abuse to order. A paedophile sitting in the United Kingdom willing to pay for this service can designate the ethnicity, age and dress of the child they want to see being abused, and they can direct that abuse online in live time. That is a fundamentally different type of risk from the one we faced before. It is one we should be deeply concerned about, and we need to think of more innovative, original and disruptive ways to stop that type of offending.

You asked about legal powers. I would be more than happy to come to that later. I am conscious that you want reasonably pithy comments to start us off. Of course, being pithy does not come naturally to the Irish.

The industry could do a number of simple things, but we need fundamentally to reset our definition of success in protecting vulnerable children, so that we are not looking at definitions of success based on finding and reporting more offending to the criminal justice system and prosecuting more offenders. As an institutionalised cop, I am always happy to take more people to court, but we should be defining success as our ability to prevent offending in the first place, with the same technology that is being used by offenders to target, groom and abuse our children, and stop thousands of kids becoming unnecessarily subject to that vile abuse. I will end on that point. I am more than happy to go into detail on any of those points later.

The Chairman: Thank you for your vital work in this critical area.

Mr Donald Toon: I am the director in the National Crime Agency responsible for economic crime and cybercrime. There are two direct links to some of the issues that the Committee wants to cover.

I want to pick up the previous comments on internet content. One of the fundamental issues from my perspective is the use of online capability as a specific tool to target UK businesses, individuals and the public sector, either to damage their ability to operate, or to make money by locking organisations out of their data using ransomware capability or by using online currencies to carry out a form of extortion directly online.

A range of issues are specifically important from a UK perspective. One of them, which Steve Kavanagh alluded to, is the break in the direct geographical relationship between the criminal and the victim. It is fundamentally a worldwide problem. Secondly, from the cybercrime perspective, there is the difficulty of cross-over between activity that is purely criminal in nature and activity that has a hostile state relationship. That is a real piece of complexity. Thirdly, that capability can become a set of commodified tools available for purchase using the dark web. People are able to develop a capability, using tools being created by top-level criminality, to carry out a series of attacks anywhere in the world and at any point in the UK. Those are some fundamental issues for us.

You asked earlier about whether the system is broken. From a cybercrime perspective, it is not that the system is broken but that it is developing. The system is trying to develop to catch up with a very fast-moving and fast-developing criminal threat. We have seen that in the scale and growth of cyberattacks and cyber incidents over the last three years. From a UK perspective, that was probably highlighted in the UK by the WannaCry attack that affected the NHS last year.

We have a very effective, strong relationship with the National Cyber Crime Unit in the NCA working very closely with regional organised crime units, and developing capability within forces to tackle cybercrime. That has to be seen in the very close partnership with the National Cyber Security Centre. Fundamentally, we have an opportunity to do some strong law enforcement activity, but there is a protection and prevention issue, which, given the worldwide nature of the criminality, is absolutely critical to our way forward. How do we use effective partnerships with major corporate operators to ensure that prevention and protection are effective?

Detective Superintendent Phil Tomlinson: I am the outgoing head of the National Digital Exploitation Service for counterterrorism policing. We provide a number of dedicated capabilities for the counterterrorism command in London, a number of support functions for wider counterterrorism policing in the UK and some support functions internationally.

We provide seven services for counterterrorism policing. There is communications data exploitation, which is the recovery of data that companies collect about individuals' account histories, cell site data, billing information and so on, which we use UK legislation to obtain. We have the open source exploitation service, which incorporates the Counter Terrorism Internet Referral Unit, which you may have heard of. It engages in the takedown of terrorist content. I am sure we will talk about that this afternoon. Since the creation of that team, we have withdrawn more than 300,000 videos, documents and speeches from the internet by working with industry, obviously collaborating very closely with our colleagues in wider policing.

The next service we provide is to do with digital media exploitation, which is conventional digital forensics. We are one of the UK’s lawful intercept agencies. We provide a technical innovation and development service that develops new software and works on decryption and advanced forensic recovery from recovered devices and so on. We have a digital biometric service that is developing new capabilities for the collection of biometrics, and increasingly using biometrics to access data. You will know from your own devices that a lot of data is no longer obtained through passwords and passcodes; it is now accessed through biometrics, so we are looking to understand that technology and apply it in terrorist investigations in the UK. Lastly, there are digital operations, which provide a lot of multisource analytics, understanding data, contextualising it and, more importantly, presenting it so that people can understand what the data means, not just for investigations but for prosecutors, courts and ultimately members of the public in their role on juries in public prosecutions.

The first big challenge for counterterrorism policing is the volume of data we collect in investigations. A typical terrorist investigation will recover approximately 10 terabytes of data. Some of the big investigations can involve between 30 and 50 terabytes. To put that into context, if you were to print it out on A4 paper, the pile would be about 100 miles high. Unfortunately, with those increasing volumes of data we do not have increasing numbers of police officers to deal with it, so we are looking for multiple pins in multiple haystacks stored in multiple parts of the world, and we need to try to piece that information together and understand it so that we can look for the evidence when we may have people in custody.

The next big challenge for us is around the encryption of data. If we are able to obtain data, we need to understand it and decrypt it. Often, the encryption changes very rapidly. Some of the bigger companies might change their encryption twice a day, which means that, if we are able to obtain information on a Monday morning, by Tuesday morning we will have to come up with a new solution to obtain the data. That is an increasing problem for us and probably takes up most of our time.

The next challenge, which I think we will talk more about this afternoon, is around social media. Social media have presented three big issues for counterterrorism policing. The first is ease of access to information about terrorist groups. In the last few years, we have seen vulnerable young people finding information online that provides advice and guidance about how to travel to foreign countries to engage in terrorist activity.

Secondly, it is very easy for individuals operating in terrorist groups to put their messages out. We have seen propaganda, beheading videos and the like broadcast on the internet in recent years. Thirdly, there is the ease of direct communication between individuals and terrorist groups. A large number of the social media companies provide messaging services. I am sure you use some of them yourselves when communicating with friends. People often ask us how terrorists communicate with one another. It is exactly the same way as we all communicate. Technology has advanced to a stage where we can communicate securely and safely, and there is no need to engage in particular forms of communication, because what is readily available on the internet for free is the type of communication that terrorist groups use themselves. Social media are probably the third biggest problem for us.

Next is the pace of technology. I touched on that with encryption. Technology is constantly evolving. We find it harder and harder to obtain information that we can use evidentially and engage in prosecutions. We work collaboratively with our partners to obtain as much of that information as possible, and use it collectively to help keep the UK safe.

The internet referral unit has been in existence for eight years. As I mentioned earlier, we have taken down over 300,000 videos. In the last week, we have removed 400 videos from the internet, so a large number of videos are still being broadcast on the internet. At our peak, 12 months ago, we were removing 2,500 videos a week. You can see the scale. It is often equated to the game whack-a-mole; we are constantly trying to identify where images are popping up on the internet and remove them.

We use a number of tools and processes, but, most importantly, we work very closely with those in the industry to try to educate and inform them about the risks of radicalisation, particularly in young people. The style of some of the videos being used over the last 12 months by terrorist groups is clearly targeting vulnerable young people who play games such as "Call of Duty", to make it look familiar to them. They are very slick and professional videos that are very appealing to young people. We are working with industry to make sure they can recognise such videos and remove them as quickly as possible.

With some of the bigger companies, we look to remove videos within 20 minutes. We estimate that, if we can remove the video within the first two hours, it will have a significant impact on the availability of that video globally. We think that after two hours the chances are that the video is out there; it has been downloaded and captured, and stored on people's devices, so we have less impact. That is not to say we will not continue to try to remove those videos and look for them elsewhere on the internet. We are very mindful of the pace at which we need to operate, and that we need to educate companies and industry so that they can work with us, realise the risks and have processes in place to remove material as quickly as possible and, importantly, prevent it being uploaded again.

Those are the key issues for us. I am happy to answer more detailed questions about any of those areas.

The Chairman: I thank all of our witnesses for those introductions, which we are now going to pick up in a series of questions.

Q36 **Baroness McIntosh of Hudnall:** It is quite hard to take in everything you were saying, so this question might seem incredibly narrow, given the breadth of what you have all just offered us. All of you talked about working with the industry. Presumably, in relation to the videos you describe you work with YouTube, or whoever facilitates, by existing, the uploading of material.

To what extent are those platforms and companies protected by the e-commerce directive and do they have the safe harbour protections around them? In view of the fact that you work closely with them, you could obviously say that they are doing all right and they are not hiding behind that. At the same time, however, they have protections. Is it your view that the time has come for those protections to be changed or repealed?

Ms Susie Hargreaves: In relation to child sexual abuse, they do not have those protections under the e-commerce directive. Once notified, they are responsible for the content and must have it removed. One of the issues for us post Brexit is the loss of the e-commerce directive. It is quite straightforward in relation to our work; they do not have a place to hide. If we have assessed it as illegal, they will take it down, but they do it on a voluntary basis with us. As a self-regulatory body, we have no powers, but once they have been notified they are criminally liable for the content.

Baroness McIntosh of Hudnall: Can I emphasise the point you made in your written evidence, which is that, in the field where you work, there is no ambiguity about what is legal or illegal?

Ms Susie Hargreaves: Correct.

Baroness McIntosh of Hudnall: I imagine that in some of the other areas it is not quite so clear, but it works in your field.

Ms Susie Hargreaves: That is correct.

Mr Will Kerr: My answer is a bit more straightforward; it is yes. Now is the time to revisit the general protections given under the e-commerce directive. Susie is quite right; it is a bit more straightforward and binary when it comes to CSEA, but people are being trafficked throughout the United Kingdom at the moment for the purposes of sexual exploitation, and that is facilitated through adult service websites for which the hosting companies have no direct legal responsibility.

To make that real for you, very recently we had a case involving some men. One was convicted at the beginning of this year. It was a fantastic piece of work by West Midlands Police. A 14 year-old girl in Coventry had been advertised on an adult service website for £30 a month. The reason she ended up on that website is that she had been in care; she was a looked-after child with a significant range of domestic problems and had become drug dependent. She had worked up a £1,800 drugs debt. Her drug dealer sold her debt to another drug dealer, who decided that as a 14 year-old girl she did not have the means to pay, and effectively took her into captivity in a house where she was guarded by a brother of the man. There was a very effective policing response, but in the four days it took to deal with the situation she had been forced to have sex with at least 20 men for between £120 and £150. That was hosted and facilitated by some of those sites. The sites have no vicarious responsibility for illegal activity that happens on them just because they happen to be a hosting platform. That needs to change.

Baroness Bertin: You mentioned in your introductory remarks that there were specifics that certain companies could do. Could you let us know very briefly what those specifics are?

Mr Will Kerr: I am very happy to. I am happy to go into detail on any of them. Sometimes, we cannot respond to the growing demands of the problem and we have to take a fundamentally different approach. That approach should be far more preventive in mindset. What could some of those companies do around CSEA?

They could do three simple things. One is that we could start to pre-screen or pre-filter some of the material before it reaches a hosting platform. The technological ability exists to do that. A significant proportion of indecent photographs have their own hash identities; effectively, the photographs have a digital signature. The known photographs that we have exist in what is called the Child Abuse Image Database in which there are over 9 million known and graded images. Let us plug one system into another and make it clear that, if you are responsible for hosting a platform, you must stop those images being uploaded in the first place and stop them being shared, and you have a proactive responsibility to take them down. That is a very simple thing that could be very effective.

Secondly, as the parent of a 13 year-old boy who spends more time on live-streaming and live-gaming apps than I would like, I would like to see some official means of kitemarking those systems by each of the companies. Not everyone agrees with me on that, but as a parent and a consumer I want to know that, when my son goes on to one of those sites, the company has signed up to three or four basic preventive steps and agreed to those design steps when it created new apps. Language algorithms have been developed that can identify grooming conversations with children. There is a developing AI space for some companies. We constantly look to prevent indecent images being uploaded to platforms servers in the first place.

If there was some form of official kitemarking, consumers and investors could make informed choices about the companies they want to invest in. I appreciate that it is a wide marketplace. It includes everything from a set-up by a 17 year-old in his or her front bedroom to multinational conglomerates. I appreciate that I am speaking generally.

Thirdly, perhaps slightly controversially, why would it not be possible for larger companies in particular to invest a certain percentage of their research and development budgets in preventing this happening on their platforms in the first place? If we can spend a certain percentage of R&D budgets on developing the AI that we know facilitates the encryption, destruction and anonymisation software that facilitates offending, why can we not spend an equal percentage of R&D budgets to stop offenders in the first place?

Baroness Kidron: I declare an interest. I am a member of the technical working group of the WeProtect Global Alliance in which Susie is also involved. My question is for you, Susie. Picking up what Baroness McIntosh said, is not the problem about the safe harbour? If you tell them that they have a duty to take it down, but they have no corresponding duty if they are not told and they can host whatever, is that not the crux of the problem?

Ms Susie Hargreaves: That is true, because we only know what we know, if you know what I mean. Once we know, we notify and action is taken, but one of the reasons we have a blocking list is that action is taken at a very different rate across the world. Action is taken very quickly in the UK, but it is not the same across the world. You are absolutely right; we would not know. Having said that, we get referrals from industry.

Could I say something about hashing? We work very closely with the Home Office, and we assess over half a million images for the Child Abuse Image Database. We have our own hash list and the Child Abuse Image Database hash list, which we supply to industry. Unfortunately, we are limited by the terms of a letter from the Home Office to share those hashes only with a number of US companies, but those companies upload all images. If you put an image on Facebook today, it will go through our hash list. Currently, there are about 310,000 unique hashes on our hash list.

Baroness Kidron: Can you explain why it is limited, just so that we understand it?

Ms Susie Hargreaves: The reason it is limited relates to when the agreement was originally set up. There is mandatory reporting in US companies and it is linked to that. If they find things, they go to NCMEC, which Will mentioned, and the reports come back to UK law enforcement. From our perspective, we want to be able to deploy the hash list across all industries so that they can use it to stop known images being uploaded.

Baroness Bertin: The implication of that is that the referrals will rocket up and go too high. Is that why they do not want to do it? Sorry, I do not understand.

Ms Susie Hargreaves: We do not have mandatory reporting in this country, so it closes the victim loop, with reports going from US companies to US law enforcement, in relation to perpetrators and victims back in the UK, if it applies.

Baroness Kidron: There is something around “Don’t look, don’t see” and then mandatory reporting. I recognise your plea that, if it ain’t broke, don’t fix it, and the very good work you do, but there are some details around the edges that might tighten up some of the loops, or open up some of them, depending on how they fall.

Ms Susie Hargreaves: Clearly, we are covering only a teeny bit of the whole problem. The big US companies in particular have a whole range of technical services to prevent, block and disrupt child sexual abuse. Their search engines take our keywords. We have had engineers in residence from Google and Microsoft. Next week, we are attending a Facebook hackathon in San Francisco. They are very responsive to the area of work we are in. Grooming is a huge issue and the threat changes on a daily basis, but at the moment that is outside the remit of the IWF.

The Chairman: Do any of the other witnesses have anything to say before we move on?

Mr Will Kerr: The threat is changing almost on a monthly basis at the moment. We should not, particularly on the law enforcement side, be naive or complacent about the changing nature of the threat. We are struggling in terms of the capabilities we need to keep up with the criminals who are trying to exploit our children. It is now perfectly normative for a child to go into their bedroom after school and use a whole range of live-streaming applications and just live-stream their daily lives. The opportunities that that presents for offenders are fundamentally different from what existed even two years ago. We are now, on the CEOP side of the house, having to develop education packages for four to seven year-olds. We know that nearly a quarter of three and four year-olds now have access to the internet. The problem is getting younger, wider and more serious in nature and risk every single week.

Viscount Colville of Culross: Mr Kerr, you said you would like the platforms and internet companies to do more to develop preventive ways of stopping this from getting on to the net before it happens. Facebook and Google, and everybody, say they already have thousands of human moderators looking at content, and they are developing AI, yet it still does not seem to be sorting the problem. All we can do is look at this country, but do you think we should consider making it compulsory, if platforms want to operate in our country, that they contribute a certain amount of money towards preventive research?

Mr Will Kerr: A voluntary coalition is always better than a mandatory one, but the scale of the problem and the range of apps being developed by a range of different companies is such that to get any sort of consistency of response, that must be seriously considered. It is now a problem. We need to be very careful not to use hyperbole in this area, but we are deeply worried about the scale of the threat. The whole law enforcement system is struggling to cope with the scale and nature of it. If we do not do something fundamentally different now, we will end up with the threat running ahead of us in the next few years. The short answer to your question is yes, we seriously need to consider it.

Baroness McIntosh of Hudnall: The overriding question is where and how the development of these technologies is happening such that you can get left behind. It is a naive question, but, as best you can, what is your answer? Where is the fundamental work going on that allows the technology to develop at the pace it is, and who is controlling that research? Is it happening in small pockets all over the place, or is it going on inside big companies and then being exported?

Detective Superintendent Phil Tomlinson: There is innovation all over the world in respect of app development, communication development and encryption. The most success we have had is through very careful and close engagement with companies. Some of the companies mentioned this afternoon are multibillion-pound operations with endless resources and budgets, but some apps are developed by one or two people in their bedrooms and sold to those companies, or used on phones.

It is important to make that point, because some companies do not have the resources to invest in some of the technology we are talking about, but we can work with them to educate them and help them have preventive processes. There is a responsibility on some of the large multibillion-pound companies that operate out there, but there is also a piece about collaboration and education with some of the smaller companies, getting them to work and engage with us in the UK and elsewhere in the world to ensure that they are not just protecting their customers' security and privacy, but that they are aware of the risks posed by some of the messages and communications going out from some of their customers. Close collaboration, education and training has been very successful for us in counterterrorism policing.

Chief Constable Stephen Kavanagh: The point that Will raised is really important. What we tend to do, certainly with terrorism, is look at legislation after the event, after some awful tragedy. Now we have an opportunity in the cold light of day, knowing the emerging challenge we face. Legislation or changes in procedures, processes, relationships and kitemarking made in haste after something awful are always less sustainable and less thought through than the opportunity we have today.

The Chairman: I note that your fellow witnesses broadly concur. We need to move to the next question.

Q37 **Baroness Benjamin:** I declare an interest as a champion of the Internet

Watch Foundation. I would like to address my questions to Susie and Will. We know that every nine minutes a child is sexually abused online in material coming from somewhere in the world, including developing countries. Your driving mission, as you have both said, is to protect children by taking down those sites. What process does the Internet Watch Foundation employ to safeguard human rights? For example, to what extent are individuals able to appeal your decisions to place URLs on a blacklist, and what scrutiny does CEOP exercise when giving you permission to issue takedown notices?

Ms Susie Hargreaves: When we find content, we locate where it is hosted. If it is hosted in the UK, which very little content is, we immediately notify CEOP, our referrals desk, and ask for permission to issue a notice of takedown. The best way to remove child sexual abuse is to do it at source. CEOP always has to give permission for us to issue a notice of takedown to ensure that we do not disrupt an ongoing investigation. The notice to take down is issued to the company in the UK.

If it is outside the UK, which the majority of content is, it is placed on the IWF URL blocking list, which is a web blocking list that blocks at webpage level. It is supplied at network level and deployed across the world. Today, there are 7,900 webpages on the blocking list, and we added 600 yesterday.

If you try to access one of the webpages on our blocking list and you live in the UK, you will be served a splash page that gives you a number of pieces of information. It tells you why you have been blocked; that the page has been assessed as illegal content; what to do if you are worried about your behaviour; the potential ramifications of your behaviour; and what to do if you feel you have been blocked in error.

We have a formal appeals policy. Four years ago, Lord Macdonald conducted a human rights review of the IWF and made a number of conclusions, including that we were human rights compliant and subject to judicial review. We had a complaints and appeals process in place, and he recommended the engagement of an independent inspector. We now have Sir Mark Hedley, a former High Court judge, as our independent inspector to oversee any appeals. That is made clear on our website, and it is made clear if anybody contacts us. The appeal process applies across the world.

Mr Will Kerr: The IWF is an independent organisation; it is not an extension of law enforcement, so the NCA does not direct or regulate IWF activity. We provide a method of de-confliction with law enforcement. At times, there may be operational reasons why we do not want to issue a takedown notice and we work very closely with the IWF on de-confliction.

We have a very strong and positive relationship with IWF. To give you a sense of the scale of the number of referrals we get, last year, in the financial year 2017-18, we had 1,160 reports from the IWF, of which 41 related to sites within the United Kingdom. As Susie said, most of them relate to international sites outwith the United Kingdom.

Baroness Benjamin: How many requests for appeals do you get?

Ms Susie Hargreaves: Hardly any. If we get requests, often it is because the list has been deployed inaccurately by the industry member. Someone may have been blocked and it has nothing to do with us. We have had no appeals go forward in the last couple of years.

The Chairman: There has been no fundamental appeal against your decision; it is usually because of an error.

Ms Susie Hargreaves: Correct.

Baroness Benjamin: I was interested to hear you say in your opening remarks that, if it ain't broke, don't fix it. What action would impede or harm the work you are doing at present? Why did you say that?

Ms Susie Hargreaves: Because child sexual abuse is very clear in law, and we are able to assess and our judgment is trusted; we are able to remove content at a speed that is unrivalled across the world. If we had to get a court order and a judge to decide it, the content would stay up for weeks. Our view is that it works incredibly quickly. We are a trusted organisation and we can move very quickly and get content removed so that a child is not revictimised, but we recognise that that is not the same for all internet harms. Different content needs different approaches. We benefit from absolute clarity of purpose, which is backed up by UK law.

Lord Gordon of Strathblane: In your written evidence, you mention that you get no money from the UK Government, but you get between 10% and 15% from the EU. Do you think you should get money from the UK Government, or do you think it would in any way compromise your independence if you did?

Ms Susie Hargreaves: That is a very good question. We get money from the EU as part of the UK Safer Internet Centre. We are part of that, with our partners Childnet International and the South West Grid for Learning, which provide awareness-raising and a helpline.

We have traditionally always stood away from receiving money from the UK Government because of our self-regulatory status. However, we are in ongoing discussion with DCMS about what happens to that funding with Brexit. Given the percentage, we have a legal view that it would not affect our self-regulatory status, but we do not have an absolute position on it yet.

Lord Gordon of Strathblane: Another point you make in your evidence is that stuff that is harmful and should be removed from the internet should be clearly defined in law and not subject to discretionary subjective interpretation. Surely, that has been the very basis of your success. People trust your judgment and abide by it. If you start defining it in law, somebody will wriggle out under whatever regulations you have.

Ms Susie Hargreaves: With respect, we would not say that our judgment is subjective; it is objective. When we look at an image, we ask whether it meets the category A, category B or category C criteria. Category C is much more open. If we are in doubt, we take a legal opinion on category C, whereas with hate speech, or other areas of internet harm, there is a level of subjectivity that we feel does not apply to child sexual abuse. If a child is engaged in a particular sexual act, it will automatically reach the thresholds of A, B or C.

Lord Gordon of Strathblane: To put it beyond doubt, if you said what I think you said in answer to Baroness Benjamin, when you say, "If it ain't broke, don't fix it", that applies to what you are doing; you are not suggesting it as a solution to the other problems that have been mentioned.

Ms Susie Hargreaves: Certainly not. They are all very different and need different solutions. The internet industry would benefit from clarity about the different areas of internet harms. One of the reasons companies work with us is that there is absolute clarity, but I am totally not saying that the IWF solution is the right one for every type of harm.

Viscount Colville of Culross: I would like to broaden my question to abuse not just of children but of adults. We received a very interesting submission from the Australian Office of the eSafety Commissioner, which has set up a two-tier system. In the first tier, it co-operates with the platforms and they are signed up, so they have a mutual relationship, but the second tier is for those who decide not to co-operate, and they are subjected to legally binding notices and penalties. Chief Constable Kavanagh, do you think that scheme might work in this country?

Chief Constable Stephen Kavanagh: I am not aware of the system, but it appeals to me. We have talked about the hate crime, bullying, harassment and gang-grooming that is taking place on the internet, and one of the challenges we face is that there is a spectrum of harms taking place. In any system we bring in, we have to recognise that the majority of the major providers will want to create an environment where their users are safe. Are they doing enough? I do not think they are. Will suggested that a small proportion of their profits is used for R&D and creating a safer ecosystem for their users. Is that sensible? Absolutely.

The challenge we face is that, every time we address one of the harms that is taking place on the web in its broadest sense, it mutates into something different. We need the ability to work as constructively as we can with the main providers. We have heard some really good examples of how they want to work with counterterrorism; they work very effectively on intellectual property issues and child sexual exploitation. Those principles now need to be underpinned to deal with hate crime, harassment, gang behaviour and other things. Any system should recognise the opportunity to do some voluntary work, but when it is not being conducted in the way we would wish, there has to be some bite in the system, because nice conversations have not yet got us where we want to be. There needs to be a bit of grit.

Q38 **Lord Goodlad:** Chief Constable Kavanagh, could you tell us how you distinguish hate speech and other offences, where a key element is abusive, hurtful or unwanted communications, from speech that is merely offensive, if there can be "mere" offence? Secondly, what factors do you take into account when deciding whether to notify companies that they are hosting illegal content, or whether to refer a case to the Crown Prosecution Service?

Chief Constable Stephen Kavanagh: Thankfully, following the awful events, and the poor response to them, over Stephen Lawrence 25 years ago, the advice to police is that everything to do with hate crime reporting is subjective. It is not for the police to test the victim as to whether or not a middle-aged white chap or a young white woman understands what it is like to be subject to those types of crime. Clear guidance has been published by the College of Policing to make sure that the moment somebody reports that type of crime, the police understand its impact. There is a cumulative effect of hate crime. The trouble is that previously, policing tried to look at a comment, or a series of comments, about an individual in isolation. These things impact on whole communities, whether it is a Muslim community or a black community, or whether it is based on religion or anything else.

What we have tried to do in policing is not just to impose greater rigour in allowing victims to explain why something is a hate crime. Through the True Vision website and other reporting forums, including local community hate crime reporting, we have enabled people to come forward and not be judged by the police in the first instance. We try to understand what has taken place. Why did they understand they were being targeted? What has previously taken place? Who is a suspect? What has taken place on a social media platform, perhaps around tattoos, language and regalia, that might be in the background for us to understand what reinforces it?

The police are clear that we are not the arbiters of good taste. If we were, Frankie Boyle would be out of business straightaway. We try to understand why hate crimes take place. The challenge facing internet providers, service providers and the police is that they are being ignored. People do not have confidence in the system; they are not reporting sufficiently, so there is a huge gap in our knowledge about the vitriol and nastiness that takes place on social media platforms. A lot of people disengage from them. They might block people. A range of activities takes place.

For broader abusive language and distasteful conduct, the CPS has rightly set the threshold for police or criminal prosecution very high. The inappropriate and stupid comment, or inappropriate joke, that somebody used to make in a café or pub and is now published on social media is a world away from hate crime and somebody being targeted because of their difference. But the CPS is clear that it will support the police when the victim has identified that something is a hate crime and that is the motivation behind it.

We usually go through the NCA and other bodies to make sure that the process is put in place. On the whole, we do not get the same response as to child sexual exploitation or counterterrorism, but in due course, if we can identify it as a hate crime, the providers usually give us the evidence to present to a court. The CPS is supportive, but it does not want to get engaged, and it does not want us to get engaged, in inappropriate humour and distasteful issues. Our responsibility is to eliminate discrimination and identify harassment, and make sure that victimisation is dealt with at source as quickly as possible.

The level of training is a challenge. I have changed recruit training for my new officers so that they become more digitally confident in what they are expected to do. If we have a stolen car, the idea is that a crime scene examiner takes fingerprints or DNA, but in that car there are telematics systems and Bluetooth technology that will give us a far clearer indication of where the car has been and whose phone has been on while they were trying to steal it or commit a crime in it.

I do not think we should sell the hate crime piece too strongly. I am deeply concerned that we keep alive the memory and experience of what happened to the Lawrence family and black communities, because it becomes a cyclical issue. Police fall short; communities become disfranchised and angry with policing. We need to keep an eye on hate crime on the internet.

Q39 **The Chairman:** You might argue that hate speech which does not meet the threshold for hate crime is not a policing matter and is a matter of taste, so this may be an industry question. Does the industry have a consistent view when it applies its community rules, for example, about what constitutes hate speech and speech that is inappropriate for its platforms? Are companies looking for leadership in that area from politicians or policymakers? Susie, can you help us with that?

Ms Susie Hargreaves: I do not think they are consistent, because everyone has different terms and conditions. This is probably an area where some clarity will be very helpful to industry, but for lots of types of content companies have their own terms and conditions.

Mr Will Kerr: It is a very difficult space to legislate for. Separating intent in the use of language and behaviour that, as Steve rightly said, would have happened in the street, in shops and in face-to-face encounters from intent in what is now happening online—those are fundamentally different. We need to think about it very carefully.

An average 16 year-old today spends between 60% and 70% of their time communicating with another human in a virtual space; they do not do it in the way you or I may have experienced growing up—presuming you are in my age band, which is very presumptuous. We need a fundamentally different set of laws that reflect the experience of children growing up today who communicate, think, act and speak fundamentally differently because it does not involve eye-to-eye or face-to-face contact. That is a different human dynamic, and our legislative base needs to evolve to reflect it.

Lord Gordon of Strathblane: We have heard some evidence that what the Germans have done, for example, has gone slightly too far; the pendulum has swung too far in the other direction, which will inevitably produce a recoil effect. Do you agree?

Mr Will Kerr: I do not know much about the German experience, so I cannot make an informed comment on it. All I know is that, as Steve hinted, the CPS has set a sensible and necessarily high threshold for hate speech. Balancing that with the need for free speech in a liberal democracy is difficult. Of course, that is not for us as police officers; we enforce the laws that legislators set, but it is a very difficult balance, which is evolving at a pace we struggle to keep up with.

Chief Constable Stephen Kavanagh: There is a massive opportunity for companies to use AI more effectively in some of these areas—machine learning concepts of abuse. At the same time, as we were discussing earlier, we have words that we may have experienced as inappropriate and would flag up as inappropriate behaviour, but on the rap scene there are hugely abusive slang terms on social media that would mean absolutely nothing to most of us in this Room, so we need the ability to adapt.

There will not be a silver bullet. Whether or not it is the AI piece identifying blatant language, we need to be able to update it and understand it, but then it will be turned into a song format or another format. Differences between gangs used to be an argument in and around a park; now they are embedded in social media, leaving lasting antagonism between groups, sometimes in very subtle ways. That is driving violence not just on the internet but in some of our local communities.

Baroness Kidron: My question follows on from your last comment, Chief Constable. I was going to ask about the culture of the internet the other way round. We all support the high bar of criminality, but is there something in the design of services, in signing up to better terms and conditions, in moderation, in mediation and quicker response time? Is there something that companies could be doing to detoxify their own environments, so that perhaps there is not a huge push towards something that may or may not become criminal in the end? It is not putting blame on them but putting responsibility in that place. Do you feel that is the case?

Detective Superintendent Phil Tomlinson: There are things that can be done. There is a huge range of different terms and conditions and different legislation in different countries. The internet is global and there are many companies operating in different parts of the world. Some of the large US companies are very particular about protecting their freedom of expression. A video that we say is offensive and may be hate speech in the UK may not be considered to be so in the US, so there could be reluctance to remove it.

However, to go back to the point about education and information for companies, they have technology that can block access to websites from the UK. IP addresses in the UK can be blocked from accessing videos. Some stuff can be done by the companies. Even if there is no breach of their own terms and conditions, they can understand that there is legislation in the UK and technology in the UK to prevent access from the UK and protect our UK interests, even though it is accessible in the US.

Mr Will Kerr: There is no easy answer, because it is a very difficult issue. Being able culturally to translate into online communication and engagement the level of respect you would have for an individual when having a conversation with them in real time in the real world is a bit of a challenge. Phil is right. We can address the level and ease of anonymisation that sometimes makes it easier for people to hide behind virtual proxy networks, or whatever they happen to be. There is an issue about consequence, which is something that will concern you significantly. Making sure that it is harder to hide behind VPNs or a range of other technology tools to spout hate language and, on the other hand, making sure that there is a wider range of deterrent consequences are tangible things that perhaps the system could do.

Q40 **Lord Allen of Kensington:** Detective Superintendent, how do you distinguish terrorist content on the one hand and legitimate speech on the other? I am particularly interested in where the content endorses conservative religious views? What factors do you take into consideration when you are looking at whether to notify a company or refer a case to the CPS?

Detective Superintendent Phil Tomlinson: We have a number of methods to identify what might be terrorist content or extremist content online: referrals to the Action Counters Terrorism website; public referrals using the anti-terrorist hotline, Crimestoppers or a local police station; or referrals through other agencies or charities. There is a huge range of areas where people can make referrals to us to highlight their concerns about content they think may be terrorist or terrorist-related.

We also have our own processes in place where we can look across the internet and search for what we think may or may not be terrorist content. Once we have obtained information and looked at it, we compare it with the database we already have of what we know is terrorist material, either because it has been used to support prosecutions or because it has already been looked at by the Crown Prosecution Service.

We look at the terms and conditions of the company. You may click the box to say, "Yes, I've read the terms and conditions", but we are some of the few people who actually read them and go back to the company and say, "We've looked at this material. We assess it to be a breach of your terms and conditions and we ask for its removal". At the same time, if we think it has reached the threshold of criminality, we refer it to the counterterrorism division of the CPS. It is not a case of doing one or the other; we look to do both.

The CPS makes a decision on whether or not it believes it is terrorist content. We will already have captured it evidentially and obtained as much information as we can from it, and looked to enrich it with additional communications data we obtain from the company to try to identify any suspects, if they exist. It is not a case of doing one or the other; it is a case of looking collectively across the data. Do we already understand and know about the data? Is there more we can do to enrich the data? Then we work with the companies to highlight the risk to them because there is a breach of their terms and conditions or of UK legislation.

Historically, companies were keener to remove content if it breached their terms and conditions, because of the impact on markets and advertisers, than if it potentially breached UK legislation, particularly if they were based overseas and not governed by that legislation. That has improved, particularly over the last 18 months, and we now see fast takedowns by companies.

Lord Allen of Kensington: Do you see it as binary? Is it either terrorist content or not, or is the model similar to the A, B and C content model in a different environment? There must be a grey area, which is always the difficulty. Do you have any insight on that?

Detective Superintendent Phil Tomlinson: A good example would be where a major online news outlet puts out an Islamic State video. The same video could appear on a terrorist website and we would say that it had terrorist content and would look to remove it. Often, it is the context—the narrative that goes with the speech and the way it has been advertised or presented on the internet—that makes the difference between distributed and publicised terrorist material and journalistic material.

It is a very fine line, and more could be done to work with online news agencies in particular to inform and educate them on the risks of publishing such videos, which potentially reach a far wider audience than the people who find them on file-sharing sites, which might be quite obscure on the internet or could even be on the dark web. A lot can be done to work with some of the big agencies to educate them to understand the increasing risks of putting out that material.

Baroness Bertin: I should have made a declaration earlier. I work for BT.

I want to pick up a point Susie Hargreaves made about education, particularly on live-streaming. How good do you think sex education, which will be compulsory from September, is on that issue? That will be so important. Children need to understand the potential of what they are doing.

Ms Susie Hargreaves: Absolutely. It is important to raise awareness of the issue. We hear the phrase "building resilience online", but we are dealing with child sexual abuse from nought to 18. You can build the resilience of a 16 year-old, but you cannot really build the resilience of a one year-old, so you have to take different approaches.

As Will mentioned earlier, we published a report today about the use of webcams in bedrooms. We have seen children as young as three in bedrooms. Clearly, they had been coerced to take part in some really bad acts. We need to do a lot of work on the educational side so that parents and families are aware of the implications.

Baroness Bertin: Do you think schools are really aware of how serious it all is?

Ms Susie Hargreaves: Increasingly so. We are a third of the CSEA of the UK Safer Internet Centre, and we also run the UK Safer Internet Day in February of each year. Increasingly, there are great campaigns by the NSPCC and others, and there is CEOP's Thinkuknow initiative. There is a mass of resources, but the fact that it is coming into the curriculum will definitely help. The internet safety strategy will raise awareness, but there is still much more to be done.

People do not realise that children are at risk even in their own homes. One of the videos I watched was of a child of about 10 in her bedroom; I heard a parent shouting, "Dinner's ready", and a category A act was taking place. We have talked about technology, but where you have a camera-enabled device and an internet connection there needs to be education. Children need the right level of supervised access to those.

Q41 **Baroness Bertin:** You touched on resource in many of your comments. Do you have enough resource, and how sustainable is the level you have at the moment for the increasing volume of work you are all having to deal with?

Mr Will Kerr: My sense is that the resources are not looking at the problem in the round and we need to take a different approach. We have a tendency to treat the problem simply as a law enforcement problem that requires a Pursue response. That is fundamentally not working in the CSEA space at the moment and we need to be able quickly to recalibrate far more effort and investment into the Protect, Prevent and Prepare space. Using live-streaming in compulsory sex education is a very good example of how we need to involve a range of other government departments outside the traditional law enforcement space.

Under the Thinkuknow education platform, CEOP is developing a package called live skills that deals directly with live-streaming risks. It aims to do a range of things: educate children, parents and carers about the tactics used by offenders; think critically about people met online; respond to pressure and manipulation online; and deal with low confidence and self-esteem issues that can make children vulnerable in the first place. Those are not unilaterally policing responsibilities, but at the moment the system is designed such that we struggle to separate the issues that make children particularly vulnerable—although it is not just children—to online exploitation and abuse, from the criminal exploitation that fundamentally and clearly sits within the law enforcement space. We are cramming in too much responsibility, and the system is struggling to cope.

The Chairman: Chief Constable, you spoke earlier about effective co-ordination between police forces. We have just heard that there is probably insufficient co-ordination across wider society, government, schools and education. Where should that be taking place? First, is that forum obvious to you? Secondly, what about resources?

Chief Constable Stephen Kavanagh: I do not think there is sufficient co-ordination. There is a real opportunity for us to look at policing and law enforcement more broadly. We are trying to come together, whether on standards for data analytics, standards for information management or approaches to victims. At the National Police Chiefs' Council office, there are probably about 10 people trying to develop some strategic thinking. Either we place it with the Home Office and ask the Home Office to take some responsibility for these issues, or we say that the police chiefs, under the leadership of Sara Thornton, have a bridging role to play in showing strategic leadership in this area.

In the NHS model, the Caldicott principles for data management are interesting. Trying to set down something for the NHS on the strategic management of data nationally works very effectively. Where is law enforcement in establishing a similar model to ensure that we consistently apply those issues? This is a really important time for us. Either the Home Office needs to step up and take responsibility for some of the issues, or we need proper resourcing of the National Police Chiefs' Council, or some other set-up, to inform how we move forward in a more considered way.

We have witnessed the outcry over Cambridge Analytica and others. As policing moves into the digital age, it must maintain its consent; it must understand where it can go in the digital sphere with the support of the public. If it goes too far, we will lose the consent that is so important to the British policing model.

On resourcing, my force had 3,600 officers; it has gone down to 2,800 officers. In addition, we lost three-quarters of our police and community support officers. We have lost about 1,000 uniformed people on Essex streets. At the same time as we have been losing those staff, I have had to find officers to place in cyber teams and additional fraud teams, and to try to develop their skills in online investigations and work with the NCA. They come from community policing and local response teams.

At a time of reducing resource, we have had to pull resource out to start to manage some of those concerns. Policing is becoming increasingly thin and it is not dealing with community issues in the way it would wish and with the speed of response it would like; nor is it dealing with the digital sphere. Unfortunately, at the moment, if we are honest, it has all been stretched too thin, and we need to think about whether or not it is a sustainable model.

Baroness Bonham-Carter of Yarnbury: At the beginning, Detective Superintendent Tomlinson referred, in a very visual way, to searching for multiple pins in multiple haystacks. To pick up what you were just saying about the digital sphere, what technological tools can you use in law enforcement and, when you use those tools, what human oversight is required?

Detective Superintendent Phil Tomlinson: I mentioned some of the volumetrics at the start, with some of the larger terrorist investigations involving 35 terabytes of data. That is a big investigation, but typically we seize that amount per month. I talked about piles of paper. The entire British Library is 32 terabytes, so, in mainstream police investigations, we are often asking a police officer to read the entire British Library to look for evidence. We are also asking them to look in different parts of the world. Some of the books have been torn up and destroyed and we want them to put them back together again. That gives an idea of the scale of the problem the police face with regard to digital evidence and how they can produce it and understand it. That is just one investigation.

A typical police officer working in a borough will probably be dealing with 30 investigations. If we multiply the British Library by 30, we see some of the issues and challenges that the police are facing. There are no more resources to deal with it.

Baroness Bonham-Carter of Yarnbury: Presumably, you need language skills too. That is not necessarily something we are greatest at as a country.

Detective Superintendent Phil Tomlinson: Absolutely. In a lot of our investigations we are reading Arabic, so we have translators. We invest in translation tools that can assist us to triage data. The big problem for us, which I mentioned at the start, is around encryption. Sometimes, people oversimplify the issue and think you can download the content of a phone and then it is just a case of reading it as though you were reading the content of any other phone. It is not as straightforward as that. If you printed the content of your own phone on a piece of paper, you would not be able to make sense of it. The conversations you were having in a chat group would make no sense, because you would be seeing them on multiple spreadsheets. It is very hard to contextualise information and make sense of it.

Another issue is that a lot of data is not stored on devices but on a cloud elsewhere, so people no longer throw away their data. Five or 10 years ago, if your phone had 100 text messages on it, you would have to delete them. People do not delete information any more. It never disappears. They just upload it to the cloud and rent more space for 49p a year. They are collecting more and more information, which could be across 10 different devices because they upload it to the next phone, and then the next one and then the cloud. That presents lots of challenges for us.

There are tools we can use. Steve mentioned artificial intelligence. We can use that to assist in understanding what the evidence is and look for it on our behalf, but it is simply a system of triage. We still have to look at it and make an assessment, in the same way as internet referrals. We have to look at the information and make a human decision on it. It is not a case of AI finding and presenting evidence for us. That is a real challenge. Counterterrorism policing is luckier than many, but wider mainstream policing is facing challenges around that. In answer to your question, we need resources and technology.

Baroness Bonham-Carter of Yarnbury: Maybe more resource would help in developing algorithmic processes; it could help with person power.

Detective Superintendent Phil Tomlinson: It would help to some extent, but sometimes you cannot throw more resource at the problem. An interesting comment made to me last year was that more data would be seized in police investigations in the next two years than there are people in the UK to view it, so it will not be possible to view all the data. That is one of the issues we have to face. Chucking more resources at the problem is not a long-term solution. It might work in the short term, but in the medium to long term, we need smarter technologies.

Baroness Bonham-Carter of Yarnbury: I meant resources directed at developing smarter technology.

Detective Superintendent Phil Tomlinson: Yes. There are companies working on developing that technology, but they realise the value of it and, therefore, it comes at a price greater than the police can afford to pay.

The Chairman: There were some incredible superlatives in your presentation.

Baroness Kidron: We talked specifically about the resilience of kids, but that could go across the board. We have just talked about the technology available to people who are trying to tackle the problems. The Committee has been very interested in a sort of design-to-be-well, design-to-be-safe and design-for-society idea. What sparked my interest was the live-streaming example. What if live-streaming automatically came with switch-on and safety? Presumably, if people were determined to do harm, they would do it, but a lot of the low-level availability that live-streaming allows would be knocked out, or at least, there would be education pieces. Do you consider design-to-be-safe in any of your areas as a responsibility of industry, or at least as a new place where we could all look for some negotiated settlement?

Mr Will Kerr: I think Baroness Bertin touched on this earlier. The whole system needs to be fundamentally recalibrated. At the moment, the model is too focused on a reactive response to a growing demand that we cannot cope with. It is not focused enough on growing the capabilities to deal with the higher-end risk. We know the break point in that. A significant determinant of the break point in that model has to be the responsibility of industry to deal with preventable offending in the UK, and allow us to accelerate our capabilities to deal with some of the higher-risk offenders here. That is the fundamental problem we face at the moment.

The academic Matthew Falder was convicted in February this year. To give you a sense of the scale of that investigation, the NCA led an international task force. It took us four years to catch him. It involved a wide range of international partners and a range of covert capabilities that we had to develop ourselves. It still took us four years to catch him. That is one offender on one particularly horrific site, but with at least 300 victims worldwide. If we do not deal with the preventable offending side of that spectrum, we are not going to be able to deal with the likes of Matthew Falder, who pose a far greater risk of significant harm to a wide range of vulnerable victims.

Chief Constable Stephen Kavanagh: A whole series of guardian communities are springing up in and around the south-east at the moment. Every single one of them is underpinned by designing out crime with processes, expectations and regulation. We should not underestimate the fact that the communities that our children, our parents and we live in when we are not in this Room are as valid today as the ones we go home to when we are sitting in our houses. We have to make sure that those communities are based on the same principles that apply in the physical lives that we lead.

Baroness McIntosh of Hudnall: I want to ask Mr Toon about areas of criminality from which we need to be kept safe that are not of the sort that make us all feel deeply sick. Child sexual exploitation is deeply emotive and catches us all whenever it is discussed. What about issues to do with cybersecurity in other areas, such as our financial protection and the way the whole economy is vulnerable to significant disruption? We know that inside this institution we are regularly under attack. We are usually okay, but sometimes we will not be.

Are we sufficiently equipped with resources, whether legislative, technological or whatever, to look at other areas of criminality, or harm that may not necessarily be criminal, against which as a society we need to be able to defend ourselves, possibly pre-emptively?

Mr Donald Toon: You raise a range of issues, but many of the answers are very similar to the position on child sexual exploitation. A fundamental issue touched on earlier was around education. That is absolutely critical in the prevention of live-streaming vulnerability, but there is something about the wider ability to be safe and secure online, for people to have a fundamental understanding of the risks they and their families are running.

We see a specific problem from a cyber perspective. We have developed tools, communication and training so that parents can identify risks, such as the classic young teenager who moves from a very strong focus on gaming and crosses a boundary where it is no longer online gaming. They are no longer focused on, "How do I throw people out of the gaming structure that I am doing online?" They start to challenge websites and the operation of legitimate industry. We have seen a number of very significant incidents where young people have found their way into criminality because there was no educational process to identify the risk of them doing so. We have seen people slip into that form of problem.

We also have a fundamental problem around online financial safety. It is very clear to us that online-enabled fraud is currently the most common crime in the country. It is a crime we are most likely to be impacted by. It is also an area where the law enforcement response is probably most limited in its ability to be effective and impactful. Most of it is carried out from overseas; it manifests itself X million times inside the UK. Each time it is a few hundred pounds, but it is not X million separate offenders. We are talking about organised criminality on a worldwide scale, carrying out thousands upon thousands of offences, each one worth a few hundred pounds. That is a huge issue and the amount grows.

It is a huge issue for all the individuals involved; it is a huge problem from the law enforcement perspective. It is the same issue about education, understanding, ability to appreciate risk and ability to use some of the tools that are relevant in respect of child sexual exploitation, counterterrorism and hate speech. It is the ability to identify where fake websites are being used, such as those where people are defrauded of their pension pot and conned into investment structures. In all of those, there is the opportunity to use a similar set of tools around breaching terms and conditions of service for hosting websites and taking down websites.

There is a continuous process, but it has to be balanced between law enforcement, and the regulatory and control structure around the provision of hosting services, and the knowledge, awareness and understanding of risk of the public at large. The same tools and the same issues very much apply. The criminality is not of the horrific kind we have been talking about in the case of sexual exploitation, but its scale is significantly greater. That leaves aside direct cyberattack and cyber-risk. There are some real issues which it is important to get to grips with. It is important not to be too siloed. When we talk about trying to protect young people and increase their understanding, it needs to be about how we can live a safe life online.

Baroness Benjamin: In your opening remarks, you mentioned money and people being prepared to pay to see child sexual abuse online. How do they pay for it? I presume it is through a credit card. Should credit card companies have some sort of responsibility?

Mr Will Kerr: We are starting to see a slight shift in the risk factors involved with CSEA, whereby live-streaming gangs that exist to make money, a significant proportion of which are in the Far East, are engaged in CSEA. As I said in my opening comments, they are not sexually motivated, although some of them might be; in the main, they are in it to make a profit.

There are significant investigative opportunities and, therefore, significant disruptive opportunities in the fact that these are not just normal banking transactions. There is a whole range of both direct and anonymised money transfer systems online at the moment. I do not want to talk about them in too much detail, because the more they are used, the more we can, hopefully, disrupt and catch them. That is what we would like to do, but there are a number of different ways in which they transfer money at the moment.

Baroness Benjamin: What can be done about it? Surely, the organisations that are involved as far as the money aspect is concerned have some sort of responsibility, because they are dealing online, too.

Mr Will Kerr: Absolutely. Because this is very much an emerging and evolving element of the CSEA threat, what we have to do in the law enforcement space is develop a suite of standards that will help prevent it in a systemised way across the whole of the banking transfer industry. That is exactly what we are doing at the moment. We are trying to look at diagnostics across the system that would indicate small transactions.

For illustrative purposes, perhaps a 50 year-old man in Bradford is making multiple payments to the Far East on a regular basis. If nothing else, that might be suspicious. If it is, we need to understand how we aggregate all the diagnostics to do disruption through the money-transfer industry and not unnecessarily criminalise that 50 year-old man, who may have a business interest in the Far East. It is a careful balance, but there is a developing range of tools that we are engaged in at the minute. I just do not want to talk about it.

Q42 **Baroness Kidron:** One thing that keeps coming up is that, if somehow we work to smart standards, good ethics, regulated behaviour and terms and conditions that everyone keeps to, everything that is difficult will move to the dark web. We are interested to know your collective or individual views on that, so maybe you could all answer slightly different pieces of this question.

A subset is the role of encryption, which many people feel protects them from the intrusion of commercial companies in their personal lives, but perhaps presents a problem for people who are looking for things that should not be going on. Do you have any views, either institutional or personal, on the balance between law enforcement, encryption, transparency and the rights of business leaders? I know it is a very broad question.

Mr Will Kerr: There is no longer a binary distinction between the dark web and the open web, and Donald will no doubt be able to explain that far more effectively. The only point I would make, and I am sure Steve would make exactly the same point, is that the levels of encryption that are now standardised and de rigueur, and were not the case even three or four years ago, have a massive impact. The intensity of the law enforcement investigations and the resource investment we have to put in to catch the same offenders fundamentally changes the law enforcement investigative model. If we are to concentrate on risk, which is what we should be doing, we need a better way of preventing volume demand, to allow us to do that. On the distinction between dark web and open web, I defer to my colleagues.

Mr Donald Toon: The fact that we are able to reach a situation where the surface internet is a safe environment and that that potentially corrals problematic behaviour into subsidiary areas is valuable in and of itself. It starts to create greater consciousness among people that if they are moving into an area that looks like the dark web—the Onion router, or whatever kind of space they want to get into—they are making a conscious choice to move into an identifiably high-risk area. They are drawing a distinction between that and a safe operating environment.

There are about 30,000 sites on the dark web at the moment, of which probably 50% are engaged in, or facilitating, some form of illegal activity. Linked to that is the use of particular forms of cryptocurrency to facilitate payments and movements around the dark web. There is a whole range of issues about the ability to investigate, operate effectively and follow payments. It is a very long and complicated subject to get into. It is really important to make sure that we have a co-ordinated and effective law enforcement effort to tackle the dark web, and that we do so not just on a UK basis but internationally. Working with international partners is hugely important. The vast majority of developed countries face exactly the same problems and risks, and we partner effectively on the dark web.

Linked to that is the wider debate on control and regulation of virtual currencies, which are used very heavily in support of dark web transactions. They are certainly used very heavily in the purchase of a whole range of services—everything from child sexual exploitation to firearms supply, money laundering and major fraud. Currently, we have a situation where an entire financial and payment structure is not subject to the same regulations and controls as normal currency.

We have to be quite careful. There is an advantage to some extent, in that people know they are taking a risk if they get into virtual currencies, but at the moment it is important to make sure that there is more effective control in the virtual currency space and that we have a harnessed and mutually supportive international effort to investigate and share information and intelligence on the dark web. The more we can make the surface internet a safe place to operate, the more effective and targeted we can be, and the more we can encourage people to understand that the dark web space is fundamentally a risky area in which to operate. We could have a long debate, but that is probably the easiest and shortest way to cover it.

The Chairman: Are there any benign reasons why anyone would want to be on the dark web and, if so, could you briefly explain what they are?

Mr Will Kerr: Maybe a journalist working in a hostile country.

The Chairman: The assumption that everything on the dark web is in some way a problem does not work.

Mr Donald Toon: But it carries a risk. You still have a situation in which people are on the dark web because they know they are facing a series of specific risks. They are not in the dark web simply because they drifted into it.

Chief Constable Stephen Kavanagh: Donald did a really good job. We want the surface web to be safe for our children and for us to be able to do our banking and engage in social media, and we need to focus on greater understanding. I have struggled with the idea why in this country, if you are not an academic researcher or a journalist, there are reasons for having an Onion router to get into the dark web. Why would my son, or anybody else, want one of those pieces of kit in this country at this time? It is an important question for us to ask. We do not want to limit free speech and we do not want to limit people unnecessarily, but we need to understand why they want to go on to the dark web. There might be a justification for it, but we must focus on the open web at the moment because, if we try to take on too much too quickly, we will fail. We need to focus our efforts on mainstream society.

Ms Susie Hargreaves: I agree with everything that has been said. Although our remit is limited to the open web, we work within the dark web a lot because we are able to access and hash the images, and many of the images in the dark web are linked to image-hosting boards that are available on the open web.

The opposite of the dark web is that there is a real danger that we forget old technology. Last year, we saw the biggest use of newsgroups since we started. Newsgroups are one of the oldest chat-room technologies. There is so much content still out there on the open web, and we should not lose sight of it.

Baroness Kidron: Because it is a broadly held view, or at least a broadly held answer against regulation or community standards, that everything will be pushed there, do you think it is a disingenuous view? I agree that there are many decent reasons for being on the dark web, but at least you know you are in unfettered space. Do you think it is a disingenuous argument, which is quite mainstream, that if you clean it up upstairs it will all go downstairs?

Mr Will Kerr: Yes, in part. Matthew Falder is a perfect example. He, along with people who were so inclined, was able to use so-called hurtcore sites on the dark web to amplify the threat to children on the open surface internet. We need to understand the relationship between the two, as Donald explained so well earlier. Matthew Falder operated on hurtcore sites where people were able to share vile images. It was not just sexual abuse of children and adults; it was a level of degradation and humiliation they wanted to get them to engage in. Donald made the point that they had to exit the surface web to go on to the dark web to share that material with like-minded people, so the dark web has the ability to amplify the open surface threat. We need to understand that relationship a lot better.

Viscount Colville of Culross: Mr Kerr, we had an interesting submission from Leicester University. Its concern was vulnerable workers on the internet for whom working on platforms can be quite beneficial, such as sex workers. Its concern was that, if you over-regulate adult service sites, you might destroy the beneficial aspects for sex workers of being online and drive them underground. Do you have anything to say about that?

Mr Will Kerr: It is a challenge. There are a number of adult service websites available in the United Kingdom at the moment. In the United States, they have taken a slightly different approach with their FOSTA legislation, and closed down one site recently. They realised that a number of sites were facilitating the trafficking of people who may have presented as willing sex workers but clearly were not; they were vulnerable and were clearly and openly being exploited. It is a difficult balance.

Of course, you have to be careful not to take a blunt approach to some of the adult service websites that operate, technically legally, at the moment. I would argue that they are not legitimate. There is always a risk of displacement for some women to on-street activities where the risk factors might be greater. We need to be very conscious of that. My point is that there are a number of these sites with tens of thousands of adverts. If you were to type "company of young girls", on three main websites, you would find hundreds and hundreds of adverts. It is on a deeply worrying scale. They are used to traffic vulnerable young girls across the United Kingdom at the moment, principally but not exclusively from eastern Europe. We should be deeply concerned about that, and those technically legal platforms are facilitating it.

Detective Superintendent Phil Tomlinson: We have some evidence-based experience in counterterrorism that relates to the point about whether it drives activity to other areas. It is fair to say that some of the big US companies were bashed up in the media about 12 months ago because of extremist material appearing on their platforms. Those companies have worked really hard and removed a lot of that content. There have been influences that reduced the amount of extremist material online because of what is happening outside the UK, but we have seen a shift of terrorist material to other more secure platforms.

It comes back to whack-a-mole. There is no doubt that, if you start going after one company, it pops up in more secure areas, which are harder for us to reach. It is harder for us to engage with those companies, which are often based in harder-to-reach countries. Without doubt, we have to bear in mind the impact of pushing activity away from the big companies, where there are benefits in being able to see what people are doing, to more secure sites where potentially you do not see what is going on. It has an impact on the circulation of videos, but it also potentially impacts on your ability to see what they are doing and the methods they are employing to use propaganda, et cetera.

Q43 **Viscount Colville of Culross:** Mr Toon and Detective Superintendent Tomlinson, you have talked about the importance of international co-operation between police forces, law enforcement agencies and international stakeholders. Are there problems that we need to overcome to make sure that

that co-operation is ever stronger and more intense? There is a great difference in the approach to freedom of expression between America and the EU, for instance, and I would like you to address that. The second part of the question is: does the prospect of Brexit pose a problem for international co-operation between our country and the EU?

Detective Superintendent Phil Tomlinson: International collaboration is crucial. We talked about the fact that this is a global issue, not just a UK one. The internet referral unit has set up a process, a model, that works very well in the UK, and it has been replicated in a number of countries around the world. We work very closely with the EU Internet Referral Unit, where we have staff working to ensure that across Europe everyone has the same sort of process and benefits that we have developed in the UK.

We work closely with the other Five Eyes countries and internationally to educate and inform them about the benefits we have experienced in the UK. We have had some significant benefits in relation to CT in the collaboration we have had. We also work very closely with the Home Office to develop international reach with companies overseas. Working internationally is absolutely crucial to our effort.

We are fortunate in the UK that we are a bit ahead of the curve in respect of our engagement, and that is a model now being copied by other countries. We have regular visits from and meetings with our European and international partners to discuss ways of working, to make sure that everyone is working in the same way.

Mr Donald Toon: From a wider criminality perspective, the system and the underlying tools are there; they are effective and are absolutely critical for us to work effectively together. They are not necessarily specific. For example, on the cybercrime side, the European Cybercrime Centre in Europol is hugely important to our ability to operate effectively, but it is not bound by the EU itself, so it is not a Brexit-related issue. The fact is that the second largest bureau in Europol is that of the United States.

There is a very strong and capable approach in being able to engage a range of different partners. We use that alongside the Five Eyes structure on a standard basis to co-ordinate our activity in a wider range of countries. We have used it particularly on economic and cybercrime in the countries of south Asia and the far east of Europe to have an effective response and share both intelligence and evidential material. The systems and tools are effective. Fundamentally, the issue becomes one of will, and the desire to use them effectively.

Viscount Colville of Culross: Do you think Brexit poses a threat to that?

Mr Donald Toon: It is hard to see that Brexit in itself poses a direct risk. The fundamental issue is that, beyond Europe, we have very effective tools. What is important in the Brexit context is that we are able to continue to work effectively on joint action to investigate and arrest. There will be issues around the ability to be effective with partners within Europe. Capabilities such as the use of European investigation orders and European arrest warrants remain important to us. It is important that through Brexit we do not lose the ability to take action against criminals operating from Europe and affecting the UK, or UK criminals operating from elsewhere in Europe. It is important that we do not lose those capabilities through Brexit. That is fundamentally the issue around Brexit, rather than international co-operation in the round.

The Chairman: Do any of the other witnesses have concerns about Brexit?

Chief Constable Stephen Kavanagh: Donald has expressed it clearly. If there is anything that undermines our ability to produce orders or have arrest powers with our closest partners, we would need to tread carefully.

Lord Allen of Kensington: Are there any countries ahead of us from which we can learn from a legislative or regulatory perspective? Germany is a potential area; we have had input from Australia. With your international network, who is ahead of the game? If they are, what is the particular area?

Mr Donald Toon: The short answer is that there is not necessarily anyone ahead of the game. There are strengths and weaknesses in the approaches of most countries. A lot of approaches are very much tailored to the circumstances of the individual country. It is often much easier to operate and have more effective control if you are in a relatively small and tightly defined jurisdiction. What really matters is the ability to co-ordinate, collaborate and co-operate effectively.

I would not say there is any shining light to which we should all be aspiring. The truth is that the vast majority of jurisdictions are facing very similar problems and trying to grapple with them and find a way forward. The real issue is making sure that we can support each other, and that we recognise that this is a worldwide problem. We have to be able to have impact, engagement and understanding in all affected jurisdictions. We cannot do this alone.

The Chairman: I thank our witnesses very sincerely for their evidence, and for giving us so much time and being so comprehensive. Susie Hargreaves, you sent us some written evidence as well, which we appreciate. Two hours have gone very quickly, and there may be other issues you would have liked to draw to the attention of the Committee. If so, please do not hesitate to write to us with further evidence, or reading, that you think we might find useful.

Our witnesses work in some dark and disturbing areas. I am struck by the humanity that you bring to your work and the approach you take. I thank you on behalf of the Committee for all the work you do and the service you give, as well as for giving us evidence today. Thank you.

ISBA – written evidence (IRN0049)

About ISBA

1. ISBA represents the UK's advertisers. We champion the needs of marketers through advocacy and offer our members thought leadership, consultancy, a programme of capability building and networking. We influence necessary change, speaking with one voice to all stakeholders including agencies, regulators, platform owners and government.

2. Our members represent over 3,000 brands across a range of sectors, including the majority of the UK biggest advertisers and best loved brands old and new, in the private, public and third sectors.

3. ISBA is one of the tripartite stakeholders that make up The Advertising Association, which represents advertisers, agencies and media owners. We are the only trade organisation representing advertisers exclusively and play a unique advocacy role, ensuring our members' interests are clearly understood and are reflected in the decision-making of media owners and platforms, media agencies, regulators and Government.

4. We seek to:

    1. **Champion improved standards** in digital media to create a transparent, responsible and accountable market which serves the needs of advertisers;
    2. **Promote innovation in advertising** and new ways of working to improve effectiveness and ROI for advertisers;
    3. **Promote a diverse, high quality media environment**, offering choice for advertisers; and
    4. **Champion the freedom to advertise responsibly and effective industry self-regulation**

5. ISBA represents advertisers on the Committee of Advertising Practice and the Broadcast Committee of Advertising Practice - sister organisations of the Advertising Standards Association - which are responsible for writing the Advertising Codes. We are also members of the World Federation of Advertisers (WFA). We are able to use our leadership role in such bodies to set and promote high industry standards as well as a robust, independent self-regulatory regime.

6. This submission focuses on the areas of interest to our members, covering the broader areas raised by this Call for Evidence.

Regulatory Overview

7. Activity on the internet – by its nature multi-faceted and cross-sectoral - is currently covered by much legislation at domestic and international level. In short, the internet is far from being unregulated. However, we are aware that consumers perceive it to be less well regulated.

8. ISBA supports the right of consumers to have their data safeguarded and privacy respected and believes that responsible advertisers should be transparent about how and why they are using the data they collect from visitors to their sites.

9. For example, the use of personal data is governed by the Data Protection Act, which prohibits use without consent, except in exceptional circumstances. Further to this, ISBA welcomes the General Data Protection Regulation (GDPR), coming into force on 25 May 2018, which strengthens the law on data protection and privacy for all individuals in the European Union. It requires all organisations to comply with rigorous regulations on how they collect, process and store consumer data. We are working with the ICO and industry partners to ensure that our members are prepared for new regulations and have produced guides and are aiding our members with their compliance.

10. However, we believe the current draft of the e-Privacy Regulation requires a number of significant changes. We have been working with the World Federation of Advertisers (WFA) to develop constructive amendments and commentary to make the regulation workable. In short:

Consistency with the GDPR is critical for legal certainty
As companies are investing significant resources to prepare for the implementation of the GDPR, consistency with the GDPR will be crucial for legal certainty. Looking at Article 8, ISBA and the WFA recommends that the Council continues to explore further options such as introducing additional legal bases, developing a harm-based approach and introducing a `legitimate interest´ legal ground tied to an opt-out for targeted advertising. A technology-neutral, risk-based approach is a core component of the GDPR and should also be applied to the e-Privacy Regulation.

Consent needs to be genuine
ISBA and the WFA believes that user testing is an essential component of defining how, where and when privacy preferences should be expressed in order to create the best conditions for consumers to have transparency, choice and control over their personal data. In many cases, the best way to modify privacy preferences will vary depending on the context: prescriptive regulation cannot take this into account. Specifically, we therefore recommend deleting Article 10.

There should be a clear distinction between direct marketing and other types of advertising
In order to maintain a clear distinction between direct marketing and other types of advertising, the e-Privacy Regulation should limit the definition of direct marketing to communication using an interpersonal communication service of any advertising or marketing material which is carried out by the Direct Marketer itself or on its behalf and which is directed to particular individuals.

Post Brexit

11. We recognise and welcome the UK government's intent to align data legislation with the provisions of GDPR through the Data Protection Bill 2017.

12. Post Brexit we risk becoming out of alignment with Europe on data legislation as we no longer have a voice at the table on EU law. Alternatively, UK laws could be implemented which affect our compliancy. ISBA will be championing the need to remain in line with EU regulations and to remain compliant. Most significant for marketers is the impact of restrictions on the use of cookies and how this could affect or prevent interest based advertising. As such, ensuring alignment with Europe on e-privacy post Brexit is critical.

13. We would reiterate the concerns shared with the Committee previously. The UK is home to the most advanced digital industries in the world, with world leading digital advertising. More than 50 per cent of advertising spend is now on digital advertising, the highest in Europe. The UK market is 2.4 times as big as that of Germany and as big as the next three markets combined (Germany, France and Russia).

14. The UK's continuing leadership position in digital advertising will be dependent on the free movement of data between the UK and the EU and this will be contingent on the UK's ability to maintain data equivalency with the EU.

15. ISBA, alongside the WFA, continues to press the UK Government to remain in line with EU regulation in this area and to address how the interests of our advertising industry to might be safeguarded post-Brexit.

16. As such, we welcome this Committee's call for the ICO to retain a place on the European Data Protection Board following the UK's exit from the EU.

Independent Self-Regulation of Digital Platforms

17. Digital advertising has been a hugely important tool for our members and has had a transformative effect on their marketing activity. In the UK the proportion of ad revenue spent on digital is almost 50% and it continues to grow. However, we are concerned with the digital advertising supply chain in certain areas and are pushing for improvements to be made in all parts of the chain.

18. ISBA also recognises that individual members will hold different positions on the issue of tech accountability and regulation, dependent on their own social responsibility policies and differences in their business models. For many advertisers search, social media and user generated video are now vital steps on the customer journey. Many advertisers believe they have little choice but to spend with one or other of the major platforms.

19. In recent months hostile media coverage of the major technology platforms has intensified. Facebook, Google and Twitter have been attacked separately or collectively for a wide range of issues, most notably: allowing the spread of terrorist and extremist content; providing the means for interference in elections and the promotion of fake news; permitting child abuse; hosting content that is inappropriate or harmful for children; allowing hate speech and cyber-bullying; and data usage which raises privacy concerns.

20. ISBA recognises the calls for statutory intervention and the need to go further but wishes to see the self-regulatory principle applied as far as is practicable, for a

number of reasons. Firstly, regulation is emerging in a piecemeal fashion internationally (Germany's Netzwerkdurchsetzungsgesetz for example), raising the risk of unintended consequences. Secondly, rapidly changing technology and consumer habits present an exceptionally dynamic environment with which to keep pace. Thirdly, in terms of advertising, the UK's self-regulatory model delivers a blueprint for successful advertising regulation in many markets around the world.

21. Taking this into account, ISBA has called on the digital platforms to consider the establishment of an independent body to provide oversight of content policies and their implementation on their platforms.

22. Independent self-regulation could encompass some or all of:

    - Common principles and codes of conduct;
    - A common framework for content policies, with global principles and local expression;
    - Certification of policies and processes;
    - Certification and verification of filtering technology;
    - Pooled complaint handling and/or escalation;
    - Audited disclosure and transparency reporting;
    - Pre-existing Coalitions and Forums, such as the Global Internet Forum to Counter Terrorism) could also be considered within scope; and
    - Industry funding and independent, industry-wide governance.

23. We believe that by funding an independent body the platforms would strengthen consumer and advertiser confidence in meeting their – self-acknowledged – responsibility for content. Any solution would need to have the ability to work globally but that ISBA see the U.K. as being an ideal place to establish a framework that could then be replicated in other regions.

Brand Safety

24. In response to the issues emerging during 2017, ISBA have engaged Google and Facebook in talks and ensured they have met with our members in order to understand their concerns. We are committed to maintaining a proactive and robust dialogue with the digital industry to take appropriate action.

25. We welcome the announcement by Google and Facebook of additional content moderation resourcing. By the end of 2018 Facebook has promised 20,000 content moderators (up from 4,500 at this time in 2017), while Google has pledged overall staffing of 10,000 against the issue by the end of 2018.

26. ISBA can see that the substantive measures announced by YouTube in January represent a direct response to concerns expressed by advertisers here in the UK. These measures include higher monetisation thresholds, greater availability of manually vetted video content and regular transparency reporting. While not all requests have been met, Google has committed itself to quarterly advertisers updates and monthly meetings with ISBA.

27. We also note that YouTube has received certification against the JICWEBS DTSG Brand Safety principles, certifying their processes for the minimisation of misplacement against inappropriate content, while Facebook has committed to being certified against these principles by the end of 2018.

28. ISBA continues to push for much more proactive and positive vetting of content for all platforms before it is deemed suitable for brand advertising and for tighter monitoring and tougher action on inappropriate user comments. ISBA are pushing for implementation of 3rd party verification proactively to block advertising being placed against inappropriate or illegal content and user comments. Currently, Google has only committed to implementation of 3rd party verification that allows reporting of misplacement against inappropriate or illegal content and user comments after the fact.

Data Privacy

29. As set out above, the use of personal data is governed by the Data Protection Act, which prohibits use without consent, except in exceptional circumstances and we welcome the forthcoming introduction of the GDPR, which strengthens the law on data protection and privacy for all individuals in the European Union.

30. The reported use of Facebook data for targeted political advertising is deeply concerning to ISBA and its members for a number of reasons:

    - Personal Facebook data has come into the hands of third parties on a large scale without explicit, informed user consent.
    - It is claimed that the data has been used for psychographic profiling and covert, micro-targeted advertising, exploiting voters' fears and prejudices.
    - Concerns about the existence and use of this data have been public for a considerable period of time. Facebook relied on self-certification that the data had been deleted.
    - It has also been claimed that other apps, 2007-2015, have collected and distributed similar bodies of data, with inadequate controls.

31. In response, ISBA convened a meeting between Facebook and our members to seek reassurances that it will get to the bottom of the issues and any implications for the public and for advertisers.

32. In particular, ISBA has asked for a:

    - Comprehensive assessment of implications for advertisers from Facebook's announced review of apps accessing data before mid-2015;
    - Commitment to quarterly ISBA member updates focused on app review findings, GDPR measures and additional data privacy policies.
    - Monthly 1:1s with ISBA to focus on data privacy and additional advertiser asks:

Political Advertising

33. Political advertising in the UK requires greater transparency and regulation. ISBA believes political advertising should be brought within the remit of the ASA, with an appropriate funding mechanism.

May 2018

ITV, BBC and Channel 4 – oral evidence (QQ 143-151)

Transcript to be found under BBC

ITV plc – supplementary written evidence (IRN0122)

Answers to outstanding questions from the Select Committee on Communications

PLATFORM DOMINANCE

Question 8

The scale and market position of big, arguably dominant, digital platforms has been the subject of much policy discussion and media attention. Is this a cause for unease?

- There is gathering unease about the ability of traditional competition law and merger control regimes to cope with rapidly changing and innovative digital markets.

- A merger regime that blocked the Project Kangaroo online initiative between the UK PSBs, but waived through the purchase of Instagram by Facebook needs to be rethought. It simply doesn't look as though the results of the existing regime are always in the UK public interest.

- There's been a lot of talk about the ability of the merger regime to deal with products that are free, and with innovation issues in merger control. Equally concerning, however, is its ability to deal with rapidly changing markets and the extent to which sufficient account is taken of potential rather than actual competition.

- The struggle that the newspaper sector had to convince the merger authorities that the market had changed sufficiently to allow it to consolidate is salutary. It effectively had to be in very severe decline before it was taken seriously, and that can't be right.

- At the same time, we do recognise some challenge in spotting those mergers in the technology sector which are going to lead to a market tipping to a particular player. But if spotting those deals is hard then we're going to have to start to become far more active in looking for structural or behavioural remedies in key tech markets once they tip to a particular player, as they pretty clearly have.

TV-LIKE CONTENT

Question 9

What assessment have you made of the revision of the Audiovisual Media Services Directive insofar as it affects the regulation of TV-like content?

- In some respects, the revision is disappointing. For instance, there's very limited recognition of the need for a regulatory level playing field between broadcasters like ITV and Channel 4 and our major global online advertising funded competitors. There was minimal deregulation in the Directive: Broadcasters are still very intensively regulated and yet the new Directive has extended only the lightest possible obligations to so-called Video Sharing Platforms, which is, in any event, only one part of the new online competitor set. There's an awfully long way to go.

- More positively, there is potentially some opportunity in the obligations placed on on-demand TV providers to include 30% of European content in their catalogues and to ensure that that content is prominent.

- It's also interesting to see provisions that permit Member States to require players (most particularly including those online) to contribute to the production of European works or to pay into national content funds. This could also apply to providers who offer their services cross border in Europe.

Question 10

a) *What is the future role for public service broadcasting in a multi-platform, content on-demand environment?*

- In an increasingly globalised TV market, the case for nationally focussed public service broadcasting is more and more compelling.

- The public benefits of PSB are not hard to see – it continues to be one of the things that brings a divided nation together, our news services help underpin democracy, we reflect the nation to itself in a way that none of the global online entrants probably ever will. In addition to this, the PSB system provides key underpinning for the UK's creative industries and spreads economic benefit across the UK. All of our organisations have a colossal commitment to the UK as a whole – in our case nearly 50% of our UK employees work outside of London.

- It's worth considering news in particular. ITV alone invests around £120m per year in our news services and we have well over 500 journalists working on them. We invest heavily in training and in compliance. The result is incredibly high levels of consumption and trust in TV news. ITV News, for instance, reaches 19 million viewers per week. On Ofcom data 70% or more of people believe that TV news is trustworthy, accurate and impartial. The equivalent figures for social media are almost half that.

- But clearly the delivery of PSB content is likely to have to change over time to reflect the ways in which audience behaviour is changing. Linear channels still have very large audiences and still have a lot of life left in them, but clearly younger audiences are doing things differently and PSB needs to respond to that as we are doing.

- We have a good base from which to do this. ITV Hub is already on 28 platforms, we have 27 million registered users and had nearly 1 billion viewing requests in H1 2018.

b) *Should regulation be reformed to protect PSB in the UK, or should it be left to the market?"*

- The short answer is that there's a compelling case for rapid reform.

- For many years the dominant theme of media policy in the UK has been to introduce competition to the PSBs at every level of the value chain. This has created the competitive and innovative market we have in the UK today.

- But the problem increasingly will <u>not</u> be lack of competition, but rather undersupply by global players of certain sorts of UK television content which very specifically reflects the lives of people in the UK. Nowhere is this more important than in relation to accurate and impartial news from the PSBs which is absolutely critical for our democracy.

- We've got to act now in a variety of ways to ensure that the UK PSB system remains healthy and robust. This will include a demanding new regime to ensure the prominence of PSB content and almost certainly other interventions to ensure that PSB licences remain viable.

- But what the government also needs to do is be rigorous in <u>other</u> policy interventions. Perhaps the biggest immediate threat to PSB in this country comes not from global technology platforms but from the government's own proposals to consult on a possible ban HFSS TV advertising before 9pm to try to combat what we all agree is a serious problem of childhood obesity.

- The problem is that a pre-9pm ban is an analogue measure for a digital age. It mainly affects adults targeting the medium children are using less and less. But, above all, it will have a set of unintended consequences that are likely to make childhood obesity worse and not better, by moving marketing money into other forms of display media, particularly online, and into reducing the price of HFSS food and drink.

- There are an alternative set of interventions that would far more effectively tackle obesity amongst children, in part by encouraging and incentivising behaviour change, something on which ITV is very actively engaged through our ITV Feel Good initiative, support for the Daily Mile and our forthcoming vegetable advertising campaign.

- ITV Feel Good, is our biggest ever behaviour change campaign to inspire everyone in the UK to eat better and move more. Right across the ITV schedule from daytime, factual, entertainment, weather, current affairs and soaps, we are raising awareness of the dangers of obesity and we are inspiring change through fun, everyday 'health hacks'.

- ITV Feel Good kicked off on the 11th June and in its first week alone it reached 27 million adults with stories about obesity and 'eat better and move more' messages.

- In April ITV launched its own campaign to support the Daily Mile. In the five years since the Daily Mile started some 2,000 schools signed up and our aim was to super charge their efforts. Since we launched our campaign earlier this year over 2,600 additional schools have joined and over 1m children are now doing the Daily Mile each day at school. We are determined to press on to raise that number further.

- Additionally, ITV, along with its partner Veg Power, announced a major new and innovative advertising campaign to air from January 2019 to get children eating more vegetables. ITV will be providing £2 million worth of advertising airtime, including prime time entertainment family shows, and production will be funded by a unique alliance of the UK's major retailers

COPYRIGHT

Question 11

a) *Article 13 of the Copyright in the Digital Single Market Directive will place specific technological requirements for platforms. Is this the right model in your opinion?*

- Article 13 could bring modest progress for rights owners by giving them more leverage to negotiate and be paid for the use of their content by online platforms. But it’s a very modest staging post on the journey to the much more far reaching reform which is essential.

- As a rights holder we observe online platforms exploiting our IP for financial gain and then sheltering behind safe harbour protections.

- In principle, as the rights holder we should have the same choices online as we do offline. So we should be free to do a deal with a platform over the use of our IP if we want to, but we should also be free to say no and our content should not then appear or be monetised on that platform.

- If we can’t agree a commercial deal, it’s reasonable for us to expect that people won’t exploit our IP and we should be able to sue the platforms if they do under clear and unambiguous legal provisions. The difficulty is that the legal provisions are not clear and unambiguous at present and legal actions are risky and costly.

- So there should be obligations on the platforms to prevent our content from appearing on their services where we don’t have a deal. Technological requirements around content recognition are key to this and should be demanding and mandatory. The only way that these requirements will be effective, however, is if the platforms are clearly and unambiguously liable for breach of copyright where the technical methods don’t work and content slips through. This is critical to incentivising investment in effective technological requirements and potentially also incentivising licensing arrangements.

- Where content hasn't been uploaded to the content recognition system for whatever reason (perhaps because it is archive content) but it's still monetised by the platform, there should be a strict accounting to the rights holder for any money made by the platform and uploader.

b) *Who should bear the costs of developing and managing these systems? The platforms or the copyright holders?*

- Ensuring that you've acquired the rights you need and that you avoid breaching the IP of others should be a cost of doing business for online platforms. After all, the copyright protected content of others is a key input for their businesses which they exploit commercially.

- ITV has to bear the cost of buying rights in order to compete with the online platforms. We certainly can't take the view that we can include any content in the world that we want on our commercial TV channels unless that content has been notified to us in advance. We have to buy rights and not breach the rights of others, or we get sued. That is where we should be aiming to get with online platforms.

INTERNATIONAL REGULATION OF THE INTERNET

Question 12

a) *What are the risks if the UK introduces regulation without the co·operation of international partners, particularly the European Union?*

- We would start with the opportunities. At the moment every government is struggling with the same core question which is how we should properly regulate what the online platforms are doing. Interestingly, the European Commission's approach so far has been rather timid – it has consisted largely of Communications and Recommendations rather than the firm legislative approach that is now required.

- The result of that has been that Member States like Germany have moved in to create their own regimes to better combat internet harm. It's very striking that after their recent online law, it's said that one in six of Facebook's moderators now work in Germany.

- If we get this right, the UK has a unique opportunity for global thought leadership. The model we establish in the UK just might be one that gets taken up worldwide. It certainly wouldn't be the first time that's happened.

- Of course, there is always a chance that the regime that is eventually put in place by the EU is inconsistent with what we have in the UK. But frankly the best way to try to influence the outcome is to try to create a model that works. We've got a great window to try to do that in the UK now given that the current Commission and Parliament are in the final months of their terms and there will be an inevitable hiatus until the new teams arrive.

b) *What other international bodies should the UK work through to improve internet regulation?*

- Most governments globally are worrying away at how to balance the huge opportunities and freedoms brought about by internet platforms with the downside risks and problems that can come too.

- It’s vital that we collaborate and share our thinking as broadly as we can in international fora. There’s likely to be some trial and error in all of this so we’ve got to seek out experience of what works and what doesn’t as systematically as we can.

- In this context, it’s important for Ofcom in particular to continue to participate in as many international fora as it can post Brexit, particularly some of the key European regulatory fora such as the European Regulators Group for Audiovisual Media Services (ERGA). In this context, it was encouraging to see Ofcom referring in its recent report about online regulation to organising a conference for UK and international regulators who have a remit and expertise in internet issues in the first part of 2019.

16 November 2016

Law Society of Scotland – written evidence (IRN0057)

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 welcome the opportunity to consider and respond to the House of Lords Select Committee on Communication on the consultation: The Internet: To Regulate or Not To Regulate? We have the following comments to put forward for consideration.

1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

The internet continues to generate new possibilities and opportunities but also new challenges, including challenges to those concerned with regulation and protection of consumer interests across a host of areas.

However valuable the internet is, in embracing it, consumers can be exposed to risk because of the change in the business model. In moving online, the consumer did not choose to give up rights and protections and expose themselves to greater risks. Generally, they are not aware of what is "lost" or the exposure to risk.

Some, simply by circumstance, are more impacted by this change than others - those in rural areas more that in urban conurbations; vulnerable members of the community required to undertake the activity online.

Many of the potential challenges faced in a digital context arise in other contexts as well but the difficulties are compounded by the sheer scale of the online environment, the ability to capture, analyse and exploit data, including personal data, the immediacy of communications and intangible nature of entities operating in the online environment and indeed of the products they sell.
However, this does not necessarily lead to the conclusion that "the internet" needs to be regulated. Many regulatory frameworks can be applied in both an online and offline context – for examples competition law or rules governing unfair contract terms. A large part of the internet can therefore already be said to be regulated.

There is also considerable existing regulation focused specifically on digital issues. For example, the E-Commerce Directive liability regime works well; it is activity based rather than business model based. This helps to provide clarity and certainty for all parts of the ecosystem, balances rights of various stakeholders.

The better option may be not to look at "regulating the internet" but instead to test new regulation and review existing regulatory frameworks to ensure that they are applicable to digital environment. Taking a sectoral approach to regulation also guards against the unintended consequences and potential negative impact on both businesses and consumers which can come from attempting a one-size-fits-all approach to disparate areas.

Furthermore, "internet" is very broad term and covers a huge range of different stakeholders all with different models and with different roles in the overall system. This consultation focuses issues around online platforms, which are only one aspect of the internet economy. Many are viewed positively and can offer significant benefits to both the businesses and consumers they connect. Furthermore, "online platforms" are not a homogenous group: the potential harm of one type of platform may be very different from the risks associated with another.

However, regulation to promote better business practices, may prove helpful. The European Commission has proposed a Regulation on promoting fairness and transparency for business users of online intermediation services.

Recent events also suggest that regulation of social media platforms could be an area for further investigation and consideration.

However, any change or new framework needs to be evidence-based and proportionate. There is a risk that increased, or even divergent regulation will damage UK as attractive place to set up and invest, particularly post-Brexit.

2. What should the legal liability of online platforms be for the content that they host?

- Balance of interests

The crux of this issue is ensuring a fair balance of interests between the online platform, the content authors or owners, and anyone affected by that content – be it consumers/readers or natural or legal persons who form the subject of that content. This is a complex equation and policy, or political views will play a significant factor in directing where the lines should be drawn in any given situation.

- Control

Liability is usually linked to an element of control, a criterion which ties in with instinctive notions of "fairness". It does not seem just that a person or entity should be liable for something out with its control. However, in the context of platforms this raises considerations of effective control – both in terms of the extent of "ownership" of content and decision-making power and logistical questions around e.g. screening obligations.

There is already clear liability on online providers to act in certain circumstances – ie when they have actual knowledge of problem content (the so called "notice and takedown" regime). There already plenty of reports showing the amount of investment in take-down and the material that is being removed as a result. Improvements in AI etc will probably increase performance even more over coming years. This balanced regime has led to the ability for providers to invest, innovate and grow.

- Defective products

One scenario where liability arises is in relation to product sales – both tangible products and intangible ones, e.g. software downloads. In both of those situations it is important that the consumer knows who to pursue if there are problems with the goods or services they buy.

- Defamation

Another issue is where the content refers to an individual or legal person and makes false or defamatory statements about them, their products, services or business practices. Again, liability must be established to ensure access to justice and identify the person against whom a claim should be brought. However, establishing who is a primary or secondary publisher, and who should be viewed as author, editor or publisher of a particular statement, is much more complicated in an internet context. Furthermore, there is a balance to be struck in relation to protection of individual's reputations on the one hand and freedom of expression on the other. Any regulatory framework must protect this important human right as well.

Furthermore, as we noted in our response to the Scottish Law Commission's consultation on the draft Defamation and Malicious Communications Bill in relation to commercial publishers (specifically referred to in the draft bill), it is not clear whether for example an individual with say a YouTube channel with over 100,000 followers (not uncommon) receiving YouTube royalties would be considered a commercial publisher. We anticipate that there will be many examples similar to this where drawing a line between commercial businesses and private individuals is difficult. This is an example of an area where general legal rules should be applied but must be configured to take account of the internet environment.

3. How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

There is no single or simple answer to this first question and of course a wide variation in the effectiveness, fairness and transparency of online platforms in relation to moderation of the content they host. The concept of moderating content is also closely linked to questions around liability: the first must be determined before powers or duties to moderate can be properly assessed.

The processes that should be implemented for individuals who wish to reverse decisions to moderate content will depend on the nature of the content. If it relates to personal data, then many of the issues are likely to be covered by the new rules coming into force on 25 May under the GDPR.

Furthermore, as noted above duties or ability to moderate will often be linked to liability but can also impact upon freedom of expression. If you try and increase liability on providers, there is a clear and obvious danger that they will become arbiters or controllers of what we can all see. In addition to the threat this poses to freedom of expression it can also chill investment incentives and increase legal risk on providers.

There is a clear danger of unintended consequences if they decided to pursue the most prudent options.

It is not clear what other situations are envisaged and the appropriate oversight body may well depend on the nature of the issue. Without further detail, it is difficult to provide a useful response to this question.

4. What role should users play in establishing and maintaining online community standards for content and behaviour?

One option would be to create a code of conduct which users could sign up to. If they failed to comply with those standards, the platform might have a power to eject them. However, this could be difficult to monitor and enforce.

5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

As noted above, there is a danger that unduly restrictive regulation could in fact result in threats to the freedom of expression and freedom of information. At the same time, to the extent that regulatory obligations are introduced which would increase the scope of liability for online platforms in respect of content, there is a risk that this could result in a potentially negative impacting freedom of speech through a reduction in available platforms or barrier to new entrants in the market. This should be considered along with other factors in assessing how to regulate platforms.

Even if platforms are not to reduce in number, the easiest way to mitigate risk by taking a restrictive approach to what they will accept as online content and remove anything which could generate complaints or be viewed as illegal eg in respect of laws governing hate speech. This is an increasingly important topic with the European Commission publishing a communication directed at tackling online abuse and enhancing the responsibility of online platforms in September 2017. However, it may be difficult to determine what is or is not hate speech: effectively delegating this responsibility to corporate entities, with no means of appeal for those whose content has been removed, has generated concerns among some human rights advocates.

6. What information should online platforms provide to users about the use of their personal data?

The GDPR sets out a robust framework which should guarantee high levels of transparency and protection for personal data.

7. In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

Businesses should be encouraged to operate in a transparent manner where this is appropriate.

We note that the European Commission is investigating how best to encourage transparency of algorithms – a concern which has already been addressed in some EU legislation.

Use of personal data in line with the requirements of the GDPR is a good example of this. GDPR does itself include obligations on being transparent about use of automated decision-making and profiling, which might go some way towards addressing the issues around algorithms.

Of particular relevance are the rules contained in Section 4 (Articles 21 and 22) which protect individuals against arbitrary application of automated decision-making processes, which may function on the basis of an algorithm or algorithms. Similarly, there are EU rules for algorithmic decisions in relation to high-frequency trading on the stock market contained within the Markets in Financial Instruments Directive (MiFID II).

We also note that certain information which does not fall within the scope of the GDPR will be commercially sensitive or might fall within the scope of trade secrets: there is, and should be, no general rule that online platforms (or any other business) should publish every detail about its businesses processes.

At the same time, online platforms, like any other business, must comply with reporting obligations and relevant regulation including competition law. There has been increasing discussion around the intersection between data, competition law, consumer protection and privacy.[884]

This aligns with a growing trend for regulators generally to demand greater transparency regarding the factors that are taken into account where algorithms are used in making decisions or generating search results. The CMA's 'CARE' principles are being used to tackle this in the digital comparison tools sector to good effect, and it is certainly possible to apply these kinds of requirements with a common-sense approach avoids the need for disclosure of commercially sensitive or proprietary technical information regarding the algorithms themselves. Incidentally, the CARE principles are a good example of the benefits of taking a sectoral approach to regulation in the internet space.

On a broader note, openness and transparency in the context of algorithms/code will likely be helped over time as a result of increasing adoption of Free and Open Source Software (FOSS). This could be encouraged through government endorsement/support of FOSS, in particular within the education context where – anecdotally – the perception is that IT education continues to focus more on closed software, which means people are more likely to continue using this as they grow up/enter the workforce.

8. What is the impact of the dominance of a small number of online platforms in certain online markets?

A small number of online platforms in certain online markets may raise competition and consumer concerns.

If there are only a small number of online platforms in a particular market, this necessarily gives a greater level of control to that platform. There is a danger of abuse of position, particularly where the platform operator is also a goods vendor in its own right. This can manifest itself in a number of ways which centre around the ability to collect and manipulate data.

[884] We note in this regard that one of the CMA's annual plan objectives includes a project looking at the use of algorithms.

For example, a platform sells a particular category of consumer goods. It collects data on the preferences of those consumers which it can use to predict market trends. But it can also use that data to identify the best-selling products in that category at the current time. It can therefore focus on those goods, reducing storage costs for less popular products, which in turn allows it to undercut competitors using the platform. From a consumer perspective, this can lead to a reduction in the range of available products. Furthermore, it may also be used to control content e.g. where a platform sells books or magazines, it may be able to use its position to promote its own content or even influence people's political views as can be seen in some of the recent analysis of the impact of social media platforms on election choices.

9. What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

There are many benefits we are only just beginning to see from the Digital Single Market (DSM). The regulation of the networks that provide us with internet access are regulated by a framework of directives which the UK helped develop and the successor to which - the EU Electronic Communications Code - is due to come into force just after the UK exits the EU. As such the entire system of regulation of the mechanics of the internet and the access networks in particular is about to be brought up to date in the EU but the UK risks being left behind with the 2003 rules.

The UK has played a leading role in the development of these new rules (as we did with the last major update in 2003) so it is vital that the same or similar rules are implemented here, regardless of UK withdrawal: the UK should ensure it will not be left out of step with a 15-year-old set of rules that is no longer suitable for 2018.

Furthermore, the Prime Minister has announced that we would be leaving the DSM. Industry has stressed the importance of updating our legal frameworks using the work done to date on the DSM rather than starting afresh with the option of "U.S. style regulation" which some commentators have proposed.

Alignment with EU regulation could also offer practical advantages for UK businesses trading with the EU/EEA. One of the challenges for internet businesses that have a global user base is dealing with the patchwork of overlapping legislation emerging within different jurisdictions – retaining alignment would minimise the regulatory changes which businesses need to tackle as a result of Brexit. Furthermore, it is important not to discourage new businesses from basing themselves or trading here: again, maintaining regulatory convergence with EU rules/principles could be helpful to businesses looking to trade on a pan-European basis.

11 May 2018

Matthieu Le Berre – written evidence (IRN0066)

The Internet: to regulate or not to regulate.

1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

I do not believe there is a need to regulate the internet. I would further argue that, as proven by the various platforms, that it is not possible and could easily be bypassed.

2. What should the legal liability of online platforms be for the content that they host?

This is a difficult question to legislate on, as one sees the protection another sees obstruction to the freedom of speech.

3. How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

Content should not be regulated based on freedom of speech. I would encourage the reporting by the public of content and then a review by the platforms owners to ascertain the legitimacy.

It is in the best interest of the platforms to abide by the law.

4. What role should users play in establishing and maintaining online community standards for content and behaviour?

This is also a wide question, they should play the role of highlighting content that is illegal but cannot be solely decided by one report from users/members of the public.

5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

The measures should be to review reports and determine if the requests are bona fide.

6. What information should online platforms provide to users about the use of their personal data?

As per existing laws, platforms should be clear on the use and of what data is to be shared.

I would go further and say that platforms should ask user’s consent for each company they want to share data with.

If the data is only statistical and does not name individuals, consent would not be needed.

7. In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?
I do not believe that the platforms should make special arrangements to divulge algorithms.

It is for the user to decide what information is right to be shared and what information is best not to be shared on a platform.

8. What is the impact of the dominance of a small number of online platforms in certain online markets?

This has typically always been the case. It has been different companies holding dominance and when a new platform responds to a different need, it gathers users and potentially displace users from an existing platform to another platform.
I feel this is a choice by users depending on their perceived needs.

9. What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

It shouldn't have any effect. The internet is a global system that is not stopped at a specific border and thus is not and cannot be fully controlled by a state. Attempts to do so will raise awareness of solutions to bypass the controls.

11 May 2018

LINX – written evidence (IRN0055)

About LINX

1. The London Internet Exchange Ltd, "LINX", 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.

2. Established in 1994, we have approaching twenty-five years' experience engaging with policymakers and other external stakeholders in matters of Internet regulation, including regulation of content and end-user behaviour.

3. With more than 780 member organisations, including most major UK ISPs and most formerly-incumbent European operators, we believe we have highly informed expertise.

Introduction

1. The Internet is often characterised by policymakers as "the Wild West". Certainly the demonization of Internet companies by political leaders, pundits and media often has the appearance of an angry mob bearing pitchforks and flaming brands. As in the Wild West, many political leaders often seem concerned only with drumming up a posse to ride out to deal rough justice to assumed wrongdoers in black hats. There is little place in this discourse for careful balancing of competing rights, the possibility that serious wrongdoing and minor or even merely unpopular infractions are being conflated, or the social value of a system of due process and fair treatment.

2. Policy makers, including even the Prime Minister, are fond of trotting out the mantra that the "the law that applies offline must also apply online". However, in more than twenty years experience engaging in Internet regulatory policy, it is our experience that what is truly meant is that the *restrictions and prohibitions* that apply offline must also be enforced online – and that they must be enforced by private companies. We detect no corresponding eagerness to ensure that the administration of online justice is protected by the same traditions of the independent prosecutors, tribunals and courts, nor even that private companies attempt to uphold and replicate the similar principles that underpin those institutions. Instead, Internet companies are judged solely by the speed with which they removed material alleged to violate standards that are unclear and untested, and by whether campaigning activists or politicians can find on those companies services examples of material or behaviour that outrages the public conscience.

3. In a mature, civilise democracy, it is accepted that the administration of justice balances competing interests. The public interest does not only lie in protecting members of the public from malefactors, but also in providing the public also a clear, comprehensible and predictable standard of laws by which they can regulate their own conduct. The public interest is not served only by the swiftest enforcement action, but also by a fair process.

4. The longstanding aggressive focus of political debate on achieving more vigorous enforcement obscures the need to develop a balanced and stable framework for the resolution of disputes and the administration of just decision-making concerning law enforcement in the online environment.

5. LINX therefore welcomes the broad scope of this Committee's enquiry, and hopes it will provide an opportunity to reflect on what kind of society we want to build in the Internet age, and what framework of responsibilities for the State and private companies would bring that about.

6. In this submission, we will identify some matters of principle the Committee may wish to consider, political leadership on which we consider essential to make material progress in developing a new framework.

Identification and characterisation of illicit content/behaviour

7. Policy discourse about Internet regulation is usually conducted in a piecemeal fashion, focussed on one type of illicit content or behaviour (e.g. terrorism or fake news). This committee's enquiry is a welcome exception.

8. Unfortunately, when it comes to the application of policy to real-world instances, a discussion about illegal content jumps the gun: it presupposes that the topic is, for example, terrorist content, and demands action in response.

9. In real life, a business process within an Internet company never starts with "terrorist content". It always starts with an *item* of content, and the first step is to determine whether it is indeed to be treated as terrorist content.

10. The first question faced by an actual Internet business is therefore never, "what do we do when we encounter content of type X?", but "Does this item trigger the process we follow when we encounter content of type X?". In other words, is this really X at all?

11. This remains fundamentally true even if the business accepts decisions from an outside source. You can, if you wish, outsource the decision-making on whether to apply a particular rule (such as deletion) to particular classes of content (such as terrorist content) to a third party. But you still need to decide *which* third parties, and what the scope of their authority will be (for example, that CTIRU will be allowed to designate material as terrorist, but not as contrary to our policy on abusive speech), whether a particular report did in fact come form that authority, and whether that report was made in accordance with the agreement or legal obligation to accept such reports.

12. There is no escaping the fundamental question. You can have a rule requiring suppressing X, but is this item before me X?

13. For this reason, political discourse on Internet regulation would be greatly improved if all agreed to cease to frame the question as "what should be done about illegal/illicit/harmful content", and instead frame it as "what should be done about ***reports*** (or ***allegations***) of illegal/illicit/harmful content?".

14. In other words, when making recommendations for dealing with illegal, illicit or harmful content, there needs to be recognition that whether a particular item infringes is not intrinsically known. The decision-maker, the process by which they reach a decision and the standards (including scope of rules) the decision-maker applies, all need to be identified. If these aspects are not clear, or do not stand up to scrutiny, then the recommendations are unlikely to be a useful contribution to the development of Internet regulation. And if they depart materially from the norms and practices that apply offline, then these variations should be reasoned and justified, and the pretence that they "merely implement the same law that applies offline" should be dropped.

The significance of an intermediated society

15. In many respects, the Internet is no different from ordinary, offline society. Most of the harms so frequently cited as being facilitated by the Internet are merely examples of ordinary criminal behaviour and the frailty of the human condition: the Internet's only contribution being that as well as facilitating and empowering the good, like any bare tool it also can also be used for evil.

16. There is, however, one material distinction between ordinary offline society and the Internet: on the Internet, almost any action or behaviour is wholly reliant on one or more intermediaries: the Internet access provider, the domain name registry, the web site or social media platform, the search engine etc. In the offline world, an actor can frequently act on their own, and are alone accountable for their action. In the online world, if a necessary intermediary chooses to intervene to suppress the action, the actor is sanctioned.

17. The legal-social model in the offline world, at least in the United Kingdom, presumes freedom under the law. An actor is capable of acting freely, and unless the law prohibits a certain action he will not face "law-enforcement" constraints. A member of a free society practically enjoys the freedom that the law allows.

18. By contrast, in the online world, when the Internet industry as a whole is forced by political pressure to intervene to suppress not only that which the law prohibits, but also that which political leaders state "any responsible company must act against", the ordinary public no longer enjoy their full measure of legally permitted freedom. In a sense, the law has changed, to become more restrictive.

19. In practical effect, online freedom is no longer protected by the principle of freedom within the law, but rather by the practical difficulties Internet intermediaries have in complying with and enforcing such political directions.

20. Maybe greater restriction is desirable. In some cases, this is very probably true. But if the democratic organs of society took responsibility for those changes, their working methods and tools (legislation) would provide ancillary benefits of public interest: fore notice, specific rules with codified and knowable scope and limits, the opportunity to challenge compatibility with human rights norms, and more. When such changes are introduced through changes in corporate policy, these benefits can be hard to realise. And that is quite apart from the intrinsic value that lies in having enforceable rules determined democratically.

Legal exceptions and justifications

21. If our aim is to ensure that the law applies online as it does offline, that means applying not only the headline prohibitions, but also the limitations of scope, exceptions and legal defences to those same prohibitions. Failure to do so would result in the scope of the prohibitions being effectively extended in the online environment or, to put it another way, freedoms being restricted that Parliament sought to protect.

22. Political pressure on on private companies demands rapid enforcement action, and usually deems enforcement of the law a *minimum* requirement; indeed, much political discourse assumes that merely upholding statutory prohibitions falls below the minimum requirement, and that any responsible Internet company ought to go much further in the "protection of the public", or lose its license to operate.

23. We do not deny that companies will often want to place restrictions on the use of their service that go well beyond legal requirements. It is perfectly legitimate for companies providing a shared communal space for their user community to want to regulate that so that it provides a welcoming and enjoyable user experience. We certainly do not want to suggest that any member of the public has the right to use any Internet-based service in any lawful manner, free from any form of restriction or limitation by the operator of that service.

24. At the same time, we must recognise that when the Internet industry as a whole responds to political pressure to be much more restrictive than the law requires, this effects a qualitative change in the impact of the law in question, as a tool for regulating social behaviour.

25. We will draw on two examples to illustrate this point, one drawn from the criminal law, and one from the civil. In both cases, the examples relative to activities/infringements that can take place wholly online.

26. In the criminal sphere, Parliament establishes precise boundaries to prohibited expressive conduct. Not only does this better guide the public and allow people to regulate their behaviour, it also carefully balances competing interests. Occasionally, such bounds are matters of great political controversy, and for private companies to ignore them (or for law enforcement and companies to collude in so doing) would be to give great disrespect the democratic process.

    a. For example, in the debates in Parliament about the extension of the law prohibiting incitement to racial hatred so as to also criminalise incitement to religious hatred, there was passionate discussion about whether this would unduly chill freedom of speech, both in the form of proselytizing and of legitimate criticism of religious dogma. Ministers answered that the Bill did not prohibit incitement of hatred against a religion (which is an idea), but against people defined by their adherence to a religion – and said that this is a crucial distinction. Moreover, Ministers argued, no prosecution can proceed without the consent of the Attorney-General, which is a powerful procedural tool for ensuring that the new law did not become a blasphemy law by the back door.

b. In the Internet context, however, politicians regularly demand that Internet companies act against "hate speech", an undefined category that includes, but is certainly not limited to, incitement to religious hatred as defined in English law. Many companies prohibit "hate speech", with no further definition, in their terms of service. And the reports they receive, demanding suppression of instances of alleged violations, are certainly not limited to those that have been approved by the Attorney General.

c. What price, then, Parliament's passionate debates and careful compromises? Are these of no lasting importance? Is it that Parliament did its job by creating a law, but the baton is now passed to companies to take it much further? Are the prohibitions that Parliament enacts of vital importance to apply to Internet communications, but the exceptions and limitations of scope that Parliament also enacted merely a trivial matter easily dispensed with? And if not, how are companies supposed to apply such limits? Are they supposed to step into the shoes of the Attorney General, and second-guess what would be seen as proportionate? For that matter, are companies supposed to tolerate heated and intemperate attacks on a religion, as long as they are clearly targeted only to that religion's ideology and dogma rather than its adherents? When are companies free to go beyond the law, and when ought they to seek to replicate its effects? These are not easy questions, but the answer "Companies must prohibit their users from doing or saying anything Parliament has prohibited, but need not pay any attention to the limits to those prohibitions or the freedoms Parliament has protected" seems unsatisfying as well.

27. For an example from civil law, consider the regulation of the use of trademarks in domain names.

a. In the context of trademark infringements, it is usually an infringement to use a registered trademark in the course of business without authorisation. However, while not everybody immediately recognises that this is an unduly simplistic description of trademark law, nobody would really think that this prohibits a ratings service like *TripAdvisor* (or, indeed, longer-established variants on the same theme, like *Which?*) from referring to trademarked brands in critical reports, notwithstanding that TripAdvisor and Which? are both doing so in the course of business.

b. The Internet, though, regularly throws up further challenging examples. DNS domain names are an essential resource for anyone seeking to offer services online. Registration of a domain name is entirely dependent on a particular kind of Internet intermediary, the domain name registry.

c. Domain name registries quickly encountered the following question: is it acceptable for a disgruntled customer to register the domain EXAMPLEBRANDNAME.COM (where "EXAMPLEBRANDNAME" is a registered trademark), for the purpose of running a website disparaging the company that trades under that trademark? What about "EXAMPLEBRANDNAMESUCKS.COM" ?).

d. Some domain name registries have developed their own system of private law that attempts to approximate, but not replicate, trademark law. Nominet (which operates the domain registry for domains ending in **.co.uk**) has its Dispute Resolution System. ICANN, which sets the policy for a wide range of domain registries, including the registry for **.com**, has its Universal Dispute Resolution System. Each applies its own systems of standards and sanctions.

e. Each of these dispute resolution systems has been criticised as being overly favourable to trademark owners, both by being overly restrictive of unregistered use (i.e. taking action to suppress unregistered use that a trademark court would not act to suppress) and by being excessively punitive (i.e. following a trademark owner's complaint about misuse of a domain, being willing to transfer the domain name into the ownership of a trademark holder in circumstances where a court might award a less draconian remedy, such as a small monetary award or even an undertaking to refrain from further infringement).

f. Ought DNS Registries to seek to replicate, rather than merely approximate, trademark law? If a domain registrant can show that a court would not seize his domain and transfer it to a trademark owner, should a Registry exercise similar restraint? Or do only some parts of the law apply online?

Evidence and context

28. The previous sections showed that there is often no clarity as to whether an Internet intermediary should seek to replicate the effects of the law as it applies offline, in all its complexity and careful balances of legitimate competing interests, or whether companies should simply aim to suppress the mischief such laws aim to prevent, without too much care for the interests of the accused.

29. In this section, we shall argue that even when there is agreement as to the meaning of the law, an Internet business is frequently incapable of applying it in a manner even broadly equivalent to the way it would be treated by a court.

30. When a court – or even a law enforcement agency, or some other administrative body or tribunal – considers an allegation, they take account of the evidence. The context in which that evidence occurred may well be relevant.

31. When an Internet intermediary is faced with a report alleging wrongdoing, that report is more closely analogous to an indictment than to evidence. It is, at best, one presentation of some of the facts. The business has no ability to call for more evidence, and little capacity to question what is there (even when so minded). In many cases context will be entirely missing, and the context will very often be sparse and misleading.

a. For example, social media platforms are often called upon to adjudicate accusations of harassment. In so doing, they will have before them one message, or perhaps one series of messages, between the parties. In most cases, they will have little idea of previous context and no ability to discover further background – and no capacity to adjudicate it if they did. In this context, harassment (which properly describes a sustained and abusive pattern of behaviour) quickly devolves into "he/she called him/her a mean name". When dealing with common patterns, such as bullying between school-age children or students, the likelihood that the complainant is truly the victim rather than the perpetrator gaming the social media platform's systems to inflict further pain is not a great deal higher than even.

b. This is not to say that social media companies should not have rules against harassment, or that they should not act on complaints of abuse. It is, however, to say that expecting to rely on social media platforms as a solution to the phenomenon of bullying or adequate protection for victims of harassment is profoundly mistaken. On the contrary, even to describe them as "having an important role to play" creates quite unrealistic expectations about how such companies can adjudicate disputes or meliorate social problems. It would be better to recognise that the extent of their capability barely even extends to being able to protect the integrity of the environment of their own service.

32. To give a very different example, consider the phenomenon of "fake news".

a. Since free societies such as the United Kingdom do not actually criminalise the publication of statements, opinions and characterisations of news events that someone believes to be untrue or misleading, perhaps the closest legal analogy is defamation. A court hearing regarding defamation will not be limited to consideration of the article that is the subject of the case; there will also be evidence about it, and about the parties.

b. Social media platforms are under intense political pressure to "combat" so-called "fake news". Let us set aside questions as to what would really constitute fake news (the committee can consider that as belong to the section immediately above, which could probably be expanded to a book-length treatment were we to attempt to deal with that category comprehensively), and also setting aside whether the real concern is State-on-State psychological warfare (and whether that is not more properly a matter for national counter-espionage agencies than multinational social media websites), and consider only the verification of news. What would social media sites need to do to be able to make even a credible effort at verifying whether a particular news item was correct? Would they need to be able to compel evidence, like a court? Would they need to have on-site reporters, who took evidence from multiple sources, like a news agency? Would they have to go further than merely marking something as "approved" or "fake", into publishing their own opinion so as to get the requisite level of nuance?

33. In this context, it's worth noting that the New York Times ran an editorial on 21st April 2018 discussing fake news on Facebook, in which it proffered the headline "*Palestinians Pay $400 million Pensions For Terrorist Families*" as an example of "far-right conspiracy programming" demonstrating that Facebook was rife with fake news. The NYT subsequently retracted this[885], after Jewish magazine Tablet, amongst many other, pointed it to the well-documented financial support programme the Palestinian Authority runs for the families of persons incarcerated or killed by the state of Israel[886].

[885] https://www.nytimes.com/2018/04/21/technology/facebook-campbell-brown-news.html
[886] http://www.tabletmag.com/scroll/260453/all-the-fake-news-thats-fit-to-print

Proportionality, total enforcement and law enforcement by algorithm

34. Once a decision has been made that a particular item matches the description given to it, and is illegal, what should happen? Should all content that is illegal be suppressed?

35. In the "offline" world, total enforcement is not the usual model. On the contrary, a great deal of discretion is available to law enforcement officers and to prosecutors about whether to take any enforcement action at all against law-breaking, and if so, whether to pursue coercive sanctions or just have "a quiet word" with the miscreant.

36. The desirability or otherwise of total enforcement is one of the (relatively few) areas where the Internet's technical features really are relevant to the policy options.

    a. Prior to the Internet, the most important forms of expressive communications that most people would engage in would be private conversations – in the home, in the workplace, in the pub. In each case, people spoke to a limited audience.

    b. It was neither feasible nor proportionate to attempt total enforcement of laws prohibiting certain types of expressive communications in that context; actual enforcement in such a context would be reserved for the most serious cases, such as where an abusive shouting match turned into violent affray.

    c. By contrast, a relatively small number of people had access to wide audiences, through broadcasting, publishing of newspapers and books etc. Compliance with the law was treated much more seriously by their publishers than private communications. The number of people who felt the bite of such restrictions was much smaller, and it most commonly felt in a professional context rather than their personal life (and so came with an expectation of a professional level of behaviour).

    d. With the advent of the Internet, "online" is added to "at home", "at work" and "in the pub". Indeed, "online" partially replaces those previous contexts: a great deal of the communications people would previously have done only face-to-face in those environments now takes place in the moment, online.

    e. That audience has changed somewhat too – ordinary members of the public are now capable of reaching large numbers of people for the first time. They also sometimes achieve that unintentionally or carelessly.

    f. Even for public figures and media professionals, the advent of social media has dramatically changed the context of their writing. Whereas previously a press release, TV interview or opinion column would be a carefully considered (and likely planned and vetted) statement, now 140 characters are tapped out on a phone in an instant, and sent off into the world to face perhaps widespread outrage.

37. The world is therefore wrestling with the question of how to cope with the public audiences being available to the untutored general public. Should they be held to the standards of traditional publishing? More particularly, should they be held to the standards of law that were previously usually only applied in practice to traditional publishing, even if they theoretically covered private communications? It would be ironic if the advent of the Internet led to such a marked diminution of freedom of expression.

    a. It seems unlikely that the answer to this can be as simplistic as "the same laws must apply online as offline"; for most people, in most contexts, those laws never did bite on them offline for any practical purposes.

    b. At the same time, abandoning all legal regulation of expressive communications is also utterly out of the question.

38. Perhaps the answer lies in recalling the broad discretion that prosecutors and law enforcement have always had to turn a blind eye to illegal expressive conduct.

    a. Should Internet companies have such discretion? If so, how should they exercise it? What guidance should they have on when it is proportionate to intervene, and when not. And do they have a duty to disapply the law even-handedly?

    b. We may welcome prosecutorial leniency towards unwise but ultimately minor expressive lawbreaking: not every fib should be prosecuted as fraud, nor every tirade prosecuted as a cause of needless distress.

    c. But if we felt that prosecutorial discretion was being applied with systematic bias, we would feel aggrieved[887]. Internet intermediary companies are currently under no legal duty to conduct their administration of laws in an even-handed, politically-neutral fashion.

39. One option would be legal reform: the Law Commission might review the breadth of laws that can be infringed, perhaps inadvertently, online, and analyse where it was previously assumed that judgement would be exercised in their enforcement, and make recommendations for change so that these laws could be administered not by public institutions with duties to the rule of law, including judgement as to reasonableness, but by corporations with no such duties, and algorithms with no such judgement. This does not seem an easy task.

40. Another approach would be to decide that placing such great weight on private companies to administer the law is a mistake. Instead of reforming the statute book, the court system might be modernised to make it capable of administering justice for an online society. Specialist courts and tribunals are rightly not created easily, but they are created when a pressing social need for them appears: we have the Patents Court, the Small Claims Court and the Employment Tribunal. Why not an Internet Abuse Court, where cases of wrongdoing are managed

[887] And historically, have. Complaints of systemic bias in the police against the black community were a major source of social unrest in the 1980s, as was the view that the police had been politicised as a weapon against striking coal miners.

through a streamlined online process, using public APIs that enable Internet companies to refer suspected criminality for action?

41. We do not pretend to have an easy answer to these problems, but the current situation is untenable. Internet companies are already struggling with the volume of complaints and allegations, and political leaders are quite insistent that what happens today is inadequate. The largest companies are being pressured into greater investment in, and use of Artificial Intelligence – algorithmic decision-making. However, far from a magic solution, AI raises serious concerns of its own.

42. The issue of "filtering", or the algorithmic prior-restraint suppression of Internet content has special relevance to concepts of proportionality and total enforcement. An algorithm knows no compromise, understands context barely if at all, and applies its rules ruthlessly. If an article satisfies its pattern-matching rules, the filter comes down in force: it has no ability to say "this is only a minor breach, and in the context of a broader and more acceptable pattern of communication, let it pass". The computer will say No.

43. There is much that can and should be said about algorithmic enforcement in relation to how crude it is, and the manifold gross opportunities for over-blocking. Such opportunities include programming mistake (known in the industry as "the Scunthorpe problem", after primitive filtering systems that were intended to block profanities), the impossibility of fully capturing the nuances of law and social norms within the precise but unreasoning language of computer code, and the algorithm's inability to understand and take account of crucial factors such as context and intent. We assume the Committee will hear from many other witnesses on this topic. Instead, we leave the Committee with a more philosophical question: even if our robotic censorship engines had perfect accuracy in restraining criminal speech before it ever took place, would you really want a society in which there was 100% machine enforcement, all the time, without proportionality, tolerance or mercy?

44. We caution the Committee not to dismiss this question on the grounds that we are far from facing that problem. Algorithmic enforcement (filtering) is already in place in some companies, searching for some kinds of content. It is certainly far from 100% accurate, but equally it is certainly 100% enforcement, in that any and every article that matches the algorithms' pattern-matching tests is marked and treated accordingly, as "X" type of content[888].

Corporative incentives and liability

45. Courts are immune from liability for their judgements. Other tribunals can and do have limited or broad immunity. Internet businesses do not.

[888] We would qualify this by noting one type of use of algorithmic that significantly mitigates this problem. When companies use algorithms to check *stored content*, the action taken against articles the algorithm identifies as infringing can be to prioritise the article for human review, instead of automatic removal. Such a procedure cannot apply, however, for content in transmission (e.g. a message being sent, a computer file being shared) as this must happen in real time. This is a large part of why Internet access providers have resisted pressures to introduce automated network filtering.

46. On the contrary, while Internet "hosting providers" have protection from liability for content stored on them by their users until they have "actual knowledge" of that content, that protection evaporates when the company acquires actual knowledge. From that point forward, a company risks being sued alongside the user; as an entity that is easily found and has deep pockets, it may well be the primary target of such a lawsuit. This provides a further reason why an Internet company is ill-suited to administer questions of law and justice; it is not independent and even a good faith attempt to reach a fair and just decision could land it with steep financial liability. The incentive is to suppress whatever provokes a complaint, regardless of the merits, and when Internet businesses are more protective of their users than not-at-all, that is to their credit.

Answers to questions

Question 1: Is Internet-specific regulation needed

47. For the most part, the mischiefs that regulation seeks to correct are not specific to the Internet. Most of the problems people identify with content and behaviour are problems that exist in the offline context, and for which viable laws already exist. New regulation should only be introduced where there is a proven need, and a realistic prospect that the regulation would improve the situation: we do not favour the introduction of legislation merely to "send a message".

48. One area we do identify a problem is in the biased incentives Internet intermediaries face in the context of Article 14 of the E-Commerce Directive: hosting providers only have protection from liability until they have actual knowledge of the article. This places on them a strong incentive to remove material, for fear of taking liability alongside the publisher, inhibiting their ability to make a fair and independent assessment of the validity of any complaint.

Question 2: liability protection for platforms

49. Protection from legal liability for third party content is an essential part of offering an intermediary service. Without such protection, it is impossible to risk carrying material that the company itself does not consider legally safe; effectively, endorse.

50. If a platform is held liable for third party content, the platform can only permit such content as it approves. This effectively extinguishes its role as a platform for the expression of a diverse range of views and content, and reduces it to a single-publication, akin to a magazine.

51. Accordingly, liability should only exist for content that the platform creates, selects, or promotes with endorsement.

Question 3: Platform moderation

52. Platforms should aspire to a high level of transparency in setting out their terms of service and acceptable use policies, so that their users can know how to regulate their own conduct in conformance to those policies.

53. The largest platforms, those with a global user base and which have the largest social impact, should consider the value of voluntarily foreswearing the "freedom of contract" right unfettered and arbitrary choice as to who may use their platform, and instead hold that it is available for use by all, subject to the terms of service, and pledge to treat all users fairly in determining whether there has been a breach of those terms.

54. The specifics of what constitutes "fair treatment" of users will vary according to both the nature of the service and the nature of the moderation, but in general it refers to some form of due process/natural justice guarantees.

55. A range of specific measures could be considered by platforms, including

    a. Notifying their users if a complaint is made against them, or otherwise their account or content is suspected of non-compliance with terms of service/acceptable use policy.

    b. Informing any user found in breach which element of the terms of service they were found to have breached, and which action or content was found to have caused the breach, with sufficient specificity that the user can understand why they are being sanctioned.

    c. Granting users the right to offer a defence that will be taken into account before they are sanctioned (e.g. before their account is closed and they are banned from the platform)

    d. Granting users a right of appeal

    e. Ensuring that decision on breaches are taken by an independent person

    f. Taking measures to ensure that breach decisions are taken consistently and without bias, so that similarly situated users will be treated equally, regardless of viewpoint. The first step to doing this would be to adopt this as an objective, and to state that it was not the role of abuse management teams to promote the company's own viewpoint or values.

56. It should be noted that offering procedural "due process" protections to users in no way fetters the platform's right to determine what content is permitted on their platform, only how it acts in response to a suspicion or allegation that the rules have been broken.

57. Not all of these measures will be appropriate in all cases. For example, stronger protections might be offered when contemplated closing an individual's (or a business') entire account on a social media platform, than would be appropriate when merely removing one ephemeral communication from display.

58. Indeed, when removing certain forms of unlawful content, it will not always be appropriate to give the user advance notice.

59. Accordingly, the range of measures we suggest for consideration are intended both as a menu from which to select, and as a loose characterisation of measures that would need to be tailored to the platform's circumstances.

Question 4: Role for the user community

60. User communities can sometimes play a useful role.

    a. On large platforms, users can act as the service providers' "eyes and ears", identifying potential breaches of acceptable use for the service provider to review.

    b. In some cases, where the platform is divided into chat rooms or forums that each have a long-standing community and traditions of their own, selected members of the community can be invested with supervisory powers.

    c. Indeed, in the case of Wikipedia, the entire enterprise is largely made up of a self-governing community, with supervision from the formal organisation geared mainly towards process and mechanisms, and intervention of last resort.

61. In our view, the circumstances of different platforms, their services and their communities are so diverse that it is not useful to generalise.

Question 5: Protection for freedom expression and freedom of information

62. In our view, protection for freedom of expression and freedom of information is achieved in the first instance primarily by the wide diversity of Internet services that are available. Additional measures are needed only to correct a problem that this diversity does not adequately resolve.

63. We can identify two areas where freedom of expression and freedom of information may not be fully protected by the diversity of platforms available:

    a. In the case of a very small number of platforms, the platform is so large and success, that a person's freedom of expression might credibly be said to not be fully realised if they are not able to access a particular platform, because that is where the audience is.

    b. When legislation, court orders, industry collaboration or government and other political pressure intervenes to ensure that the Internet industry generally follows one set of norms, then a competitive range of platforms does not suffice: the aggrieved user cannot simply go to another service provider because they must all act similarly in the relevant respect.

64. In our view, protections for freedom of expression within a particular platform are best achieved by commitments to transparency and lack of bias (discrimination either on the grounds of immutable characteristics or viewpoint), together with the possible adoption of certain due process mechanisms when considering suspicions of abuse/unacceptable content or behaviour.

65. We set out some suggestions for consideration in response to question 3.

Question 6: Personal data

66. GDPR introduces very substantial and indeed onerous new requirements in relation to the use that may be made of users' personal data, and how users should be informed about those uses.

67. We do not think that any further requirements should be contemplated at the present time; better first to wait and see the effect GDPR proves to have in practice.

Question 7-8

68. No answer.

Question 9: Impact of leaving the EU

69. Article 15 of the E-Commerce Directive, which states that Internet intermediaries may not be placed under a "general duty to monitor" has never been properly transposed into UK domestic law.

    a. Successive UK governments have taken the position that this was not necessary, on the grounds that no UK law does place intermediaries under such a monitoring obligation.

    b. Nonetheless, the lack of such transposition leaves UK operators exposed to the risk that law may be interpreted to allow the imposition of such a duty. This is particularly severe in relation to laws that grant courts a broad discretion to impose poorly identified duties on third parties, e.g. s94A of the Copyright, Design and Patents Act.

    c. While the UK was a member of the European Union, UK providers had the comfort that even though Article 15 had not been transposed, UK courts were still under a duty to act in compliance with EU law.

    d. When the UK leaves the EU, this comfort is diluted (or removed, depending on transition provisions).

70. The protection from a duty to monitor is part of the core *acquis* underlying Internet regulation in the UK and EU. We recommend that the government proceed to transpose Article 15, with prospective effect, as part of the preparations for leaving the EU.

17 May 2018

Professor Sonia Livingstone and Tony Stower, Head of Child Safety Online, NSPCC – oral evidence (QQ 71-82)

Tuesday 19 June 2018

Watch the meeting

Members present: Lord Gilbert of Panteg (Chairman); Lord Allen of Kensington; Baroness Bertin; Baroness Bonham-Carter of Yarnbury; The Lord Bishop of Chelmsford; Viscount Colville of Culross; Lord Goodlad; Lord Gordon of Strathblane; Baroness Kidron; Baroness McIntosh of Hudnall; Baroness Quin.

Evidence Session No. 9 Heard in Public Questions 71 - 82

Examination of Witnesses

Professor Sonia Livingstone OBE, Professor of Social Psychology, London School of Economics; Tony Stower, Head of Child Safety Online, NSPCC.

Q71 **The Chairman:** Can I welcome the second set of witnesses giving evidence to us today in our inquiry into regulation of the internet? Our witnesses are Professor Sonia Livingstone and Tony Stower, and I will ask them to briefly introduce themselves in a moment. Just so that our witnesses are aware, the session today is being transmitted and broadcast online, and a transcript will be taken for the record and for use by the Committee in the future. Sonia Livingstone is well known to the Committee and is very welcome and, Tony Stower, you are very welcome indeed. Thank you for coming and giving us evidence today.

Maybe you would both start by briefly introducing yourselves and telling us a little of your background. Then, just broadly, so we know where you are coming from, tell us whether it is your view that internet regulation needs to move forward, whether there needs to be some bringing together of internet regulation, whether there needs to be a new regulatory framework for the internet in its broadest sense and what form that kind of regulation best takes. Is it directed regulation, co-regulation or self-regulation? If you could address that in your opening remarks, I will then open the meeting to other members of the Committee.

Professor Sonia Livingstone: Thank you very much for inviting me to speak to you today. I am a professor of social psychology at the London School of Economics. I am a researcher of children, families, schools and the ways in which, essentially, families and the general public access the internet, and the risks and opportunities that result. I am a member of the executive board of the UK Council for Child Internet Safety and founded its evidence group. I have variously advised on children's risks and rights to the European Parliament, the Council of Europe, the European Commission, UNICEF, this Committee and various others.

I would say, yes, something needs to be done. Everyone in all quarters is calling out for some kind of action, broadly called regulation. We must be talking about some kind of mix of types of regulation. Of course, a lot of law already applies online and has been specifically developed for the internet. There is a lot that is called self-regulation, of which I and others have become increasingly sceptical as to its efficacy, and there could be potential for a lot more co-regulation than has yet been tried and evaluated. What I see, as I hope we can talk about, is that it is a little like trying to get hold of jelly: there are a lot of different regulations, practices, norms and claims to regulation across the board, and of course the internet covers every sector of society. In addition to thinking about the right mix of regulation, we also need to think about co-ordination, so that something is cross-government and cross-sector.

Tony Stower: My name is Tony Stower and I am the head of child safety online at the NSPCC. I hope you already know that the NSPCC is one of the main children's charities in this country, fighting to end child abuse across the UK and the Channel Islands. The NSPCC's position is that there is a clear and compelling need to introduce statutory regulation of social networking sites, and app sites and games that have a social element. I am going to restrict most of my answers this afternoon specifically to social networking sites, rather than the internet as a whole. Previous witnesses have said that that is a bit too difficult to get your head around, sometimes.

In our view, we have already tried self-regulation. For the last 10 to 15 years, we have seen a number of codes of practice, self-regulatory approaches and co-regulatory approaches in some instances, which have totally failed to have any lasting impact on the protection of children online. I would make an exception to this, which is the production of child sexual abuse imagery. I know you have had witnesses from IWF here, who have talked quite persuasively about the model that works in that narrow band. I am happy to talk about why social networking sites, more broadly, need to take action on grooming in particular, but also other behaviours and offensive content.

Q72 **Lord Gordon of Strathblane:** On precisely the point you opened with there, the Internet Watch Foundation witnesses claimed when they came to us that their self-regulatory approach has worked. It is not broken; do not fix it. What is your answer?

Tony Stower: I was reading Susie's testimony this morning and it is very interesting, because that is a specific area where not only are other laws across the world broadly similar, but there is a very clear ethical and moral agreement that production of child sexual abuse imagery and material is unacceptable. Our focus at the NSPCC is on issues such as grooming, where it is clear that children are still being put at risk, but the wide acceptance of that is not quite as clear, especially in other countries.

Lord Gordon of Strathblane: Surely the answer is to make sure that there is a widespread acceptance of it, and then it would be dealt with as the other problems have been dealt with.

Tony Stower: In the meantime, children will continue to be put at risk in the absence of any firm regulation for children in this country.

Professor Sonia Livingstone: I am not a lawyer so I hesitate to contest a legal point, but I cannot see that the Internet Watch Foundation is a self-regulatory body. I was on the board of the IWF in its early years, when it was incredibly contested, unstable and being challenged on all sides. It was not until the passing of the Sexual Offences Act in 2003, which designated the IWF as a legitimate authority—I might have the words slightly wrong there—and a host of other things throughout its remit that it became an effective regulator. It takes a law that designates the authority.

Lord Gordon of Strathblane: I am simply quoting their evidence to us. They described it as self-regulatory. Other witnesses this afternoon have agreed with you that it is hardly self-regulation; it is more like co-regulation. Is a principles-based approach the way to protect children?

Professor Sonia Livingstone: I just heard your previous witnesses arguing that there were already plenty of laws that stated what children's rights to protection should be. Perhaps we could separate principles of protection from principles of regulation. I would probably refer to human rights legislation, including the Convention on the Rights of the Child, to specify what we want to protect, how we want to protect children and how we want to balance their rights to protection with their rights to privacy and to participation. The principles for the regulation that we want are principles of transparency, accountability, regulation in the public interest, evidence-based regulation and independent assessment of that regulation. In terms of how the regulation should be done, I would want to see a body that operates according to the principles of good regulation.

Lord Gordon of Strathblane: What sort of body would it be? Would it be a government body or appointed by government, or would it be an industry body with external representation? What would it be?

Tony Stower: I have views, if you would like me to jump in. The first point is that principles-based regulation is all well and good, but it depends what those principles are, what resources the regulator has and how muscular it feels in enforcing those principles. From our perspective, the regulator should be an independent body that operates on the principles of better regulation, only regulating as far as is necessary and appropriate. Of course, it needs the support and co-operation of industry, so it will need to work closely with industry, charities and academics to make sure that the principles under which it operates are appropriate, and keep up with modern technology and the threat.

It needs to be independent because there is a tendency—and I can say this as a former civil servant—for civil servants to get bogged down in the weeds when we get into regulation. It is much easier for an independent body to consult, to set its own regulatory approach and to take into account the balance that it needs to strike. It is much more difficult for civil servants, who are under the direct control of Ministers, to do that.

Lord Gordon of Strathblane: My final point to either or both of you is whether we are talking of one body here or a lot of ad hoc bodies to deal with separate and sometimes different problems that require different solutions.

Professor Sonia Livingstone: We already have quite a number of regulators in this space. That is the challenge. The Information Commissioner's Office is already becoming much more significant and powerful in this regard. Ofcom has various responsibilities, as does the BBFC, and there are others. There will have to be some way of—"carving up" sounds too negative—demarcating where responsibilities lie, even if we as a country create a whole new regulator.

In that sense, if there were a new regulator, and it could be strong, fair and operate those principles, it would be fantastic. If the same responsibilities were instead given to Ofcom, I can imagine that many would think that was also a satisfactory outcome. It is largely paid for by industry. It is trusted in the space. It does a lot of things that look very similar, in enforcing codes and so forth.

Tony Stower: You need to have a clear demarcation. If you think about it, in the financial services sector there are several regulators, at least three that I can think of off the top of my head. It is clear that the PRA, the FCA and the Financial Reporting Council have separate responsibilities. That does not mean it always works well, but I would echo Sonia's perspective that Ofcom or a similar regulator that already has the respect and the muscle would be the right place for this to sit.

The Chairman: Before we move on to the next question, Mr Stower, you referred to the role of civil servants and an independent body. We were thinking of the context of regulation based on a set of principles. What is the role for politicians? Surely it is the role of politicians to build those principles, get the broadest possible support for them, and reflect the views of society and, in the case of elected politicians, their electors.

Tony Stower: I have to say that we have not done all our work on quite what the ideal form of regulation would be, but we would expect the broad scope of the regulator to be laid down in statute and then for the regulator to determine its exact regulatory approach within that. I hesitate to bring up the regulator that I used to work for, which is IPSA, where I was head of policy and strategy for some years, but the environment there was very clear. Parliament set down the rules for the regulator and the regulator itself decided the detailed rules and the approach that it would take to enforcement. That would be the right model here.

Q73 **Baroness Bonham-Carter of Yarnbury:** I do not think we will discuss IPSA. One of our previous witnesses referred to concerns about overbroad blocking. I wanted to ask both of you what steps should be taken to ensure that there are positive advantages and things that children and young people can get off the internet, and what steps should be taken to ensure that excessive regulation does not prevent children taking advantage of what is on offer.

Professor Sonia Livingstone: This is a hard one, because on the internet we do not know how old somebody is. We can have all kinds of ideas, and we do, about what is appropriate for five year-olds, 15 year-olds or 25 year-olds but, without adequate age verification, which is how I understand the present situation, it is difficult to make age-graded offers. I imagine we are going to get into that further.

At this point, one partly has to come back to the principles of good regulation. Whoever is doing blocking or operating filters, there has to be a process of independent oversight. For a number of years, the European Commission commissioned an independent company, which was Deloitte for a while, which would do independent testing of the filters and report the percentage of under and overblocking. That set up the means by which you could have a mechanism of redress. The Internet Watch Foundation did that assessment of overblocking and underblocking in house, with legal advice, but a similar sense of independent oversight. We do not have that at the moment. We have a lot of companies making claims and no ability to discover how good any of them are, unless we do a mystery shopper exercise, which could be done. It is very hard when we are talking about trying to avoid harmful content reaching vulnerable children, but it is none the less always vital that we also think about what might be being overly blocked. I am sure Tony will talk about it in terms of children getting access to help and counselling services.

Tony Stower: You are absolutely right that it is a concern, particularly where we have been engaging in debates about age verification for pornography. This has been a big element. The NSPCC's approach is less about content and more about behaviour, so overblocking is not a concern per se. We are clear that we will only support regulation that is appropriate and, as Sonia says, follows the model of best regulation. That means that we are not trying to stop children enjoying all the benefits of the internet, app sites and games, being able to do their homework or interact with their friends. Children tell us that their use of the internet and what we would call offline are totally interwoven, and children do not really see the distinction.

We are not about intervening to prevent or change that; we are trying to make sure that children can do all that safely, without having unwanted sexual approaches from adults or being sent inappropriate material. We would expect any regulator to bear in mind the needs of users, including children, industry and the views of academics and charities, and have a continuing obligation to consult with them over the course of the regulatory cycle. It might be instructive to think a little about the other public spaces that children go in; so think about youth groups or swimming pools. Of course, there are rules of the road that we expect of children. In my day, it was dive-bombing that children were told not to do in swimming pools, but we also have lifeguards who monitor, who make sure that children are safe and intervene to make sure that one user's behaviour does not adversely affect others. That is the kind of approach we are talking about here.

Baroness Bonham-Carter of Yarnbury: I know that if my colleague Floella Benjamin was here she would want me to ask about the problem of encrypted message services. Which companies would fall within the scope of your proposed social media regulation? How do you deal with that, interactive video and so on?

Tony Stower: If we are talking about principles-based regulation, the first principle would be that services that are open to children should be safe for children to use in the first place. You could set the threshold of "open to children" wherever you like. It might be that, say, 30% of their users are under the age of 18—50% or wherever. If you are providing content and expecting behaviour that is likely to be extremely sexual, it should be behind an 18 age barrier, in our view. Encryption poses a big problem. There is no doubt that many of the internet companies are doing good things to, for instance, detect nudity on live streaming sites or detect other forms of grooming but, when they implement end-to-end encryption, it is essentially impossible to intervene, so that remains a concern. I do not think anybody has the right solution or any solution, I should say, to that at the moment, but we continue to be concerned.

You mentioned live streaming, which is an issue that we have seen with adults grooming children and expecting or asking children to, for instance, remove clothing in real time, but it is not just adults and children. We also know that lots of video chatting goes on between children. Some of that activity we should not worry about too much,[889] but children are often being exploited at these ages and they do not know it. When encryption is in the way, there is no way for algorithms to get in.

Q74 **Baroness Kidron:** I wanted to ask a very small question. Sonia expressed the problem of how we know how old the child is and you have just used the phrase "open to children". I am interested in this idea of what we know, and I am mainly asking you as a researcher, Sonia. There seems to be considerable evidence of how many children are actually using particular places. Do you both think that, if there was a regulatory framework that said, "If there are more than X children on your site, it has to be regulated or it has to be suitable for the youngest user", that would be a way forward? Would we then get smart age verification terribly quickly?

Professor Sonia Livingstone: We might. The risk is that that might get services like WhatsApp saying, "I am sorry; we are not going to have any children at all". WhatsApp has just raised its age to 16, and it is an interesting question as to whether it is the responsibility of researchers or children's organisations to show that this has now caused a problem and that they are missing out on some of the opportunities that we would want them to have. My sense is that some companies—and we have already seen plenty of companies that want the family-friendly market—would begin to make that kind of offer. At that point, it becomes really important not to say what proportion of children are among the users, because there might be so many adult users that children always remain a tiny minority, but rather to say what proportion of children are using the services.

We know from Ofcom that 24% of 12 to 15 year-olds are using WhatsApp, as from last month, so they are either lying about their age—and it is shocking that a policy framework should put children in that position—or they have now been denied something that we know they were using to chat with their friends, grandparents and so forth. What exactly lies behind that decision? In other circumstances, would other companies say that this is a market that is worth something to them? I think they would.

Q75 **Baroness McIntosh of Hudnall:** Can I follow up that last point about age-appropriate stuff and particularly WhatsApp? I can see that there is a potential danger in its having raised its age to 16. That said, it is perfectly clear to me—and I know almost nothing about any of this—that children much younger than that are using WhatsApp. Children in primary school are using it and they are creating groups among themselves. They can only do that if they are enabled in some way: first, by being provided with the technology to do it, and secondly, presumably, by being able to lie about their age. We know they are being supported by adults in that. There is an education issue there, not just for the children but for the adults, and how we teach adults what it is appropriate for children to be doing. That is the first thing.

The second thing is the point I really wanted to raise. It is not just about

[889] Mr Stower clarified that he meant that some of that activity is not of concern because it is not always exploitative.

content, but the actual design of the services themselves. Relatively anecdotally, it is possible to observe children who are using internet-based services that are not in themselves pornographic, inappropriate according to age or whatever, but are just addictive, and they spend an enormous amount of time on them and find it very hard not to. This question is about your view of the design quality of the services that are available now, and what more we can do to try to make children less vulnerable to those things. Are there ways in which children themselves are or can be involved in thinking this stuff through, so that the services are not only designed better for them, but they are able to understand what risks they run? An awful lot of this is quite top-down at the moment.

Professor Sonia Livingstone: I will respond to your comment on WhatsApp. Yes, I hope that something in terms of regulation from Government is going to be said about education, but we should take seriously the fact that children have, from a young age, adopted and embraced the chance to communicate through digital technologies with alacrity and enthusiasm. It is not just a matter of saying that companies have set certain age thresholds and we should educate children so they do not lie to get on. In a way, we have to recognise that this is a very real desire to be in touch. If I can invite us to stand back for a minute, we have designed a world in which it is now very hard for children to knock on their neighbour's door or go and play in the street. We have separated them from each other and from their extended families, and then here is a fabulous service that they have embraced to stay in touch.

I will come to the addiction point in a minute, but it is not purely and simply about keeping them off. The challenge is to regulate in such a way that you stimulate rather than kill a potential market that can provide those kinds of services, such as Facebook Messenger. I do not think they should just be for children. I think of a broadly family-friendly, public-friendly service that many other people would like to use, with some clear protections around it.

Baroness McIntosh of Hudnall: Before you go on, can I ask you to talk about how encryption works within that? The fact that you cannot see what is going on when services are encrypted means there are inherent risks, does it not?

Professor Sonia Livingstone: It is a coincidence that WhatsApp encrypts. It is the only service in popular use that does. I do not think any of the people we are talking about using it care that it encrypts. It does not encrypt for them and I do not think children are calling out for an encrypted service, so maybe there could be another service. I gather that WhatsApp encrypts for the same reason that it raised the age of use to 16, which is that it has a privacy ethos that means it does not want to have to collect data or be responsible for people's personal data at all. Maybe WhatsApp has just argued itself out of the market.

I would prefer to call it a kind of compulsion and fascination, rather than addiction. You have heard me on this subject before. The clinicians are arguing about whether it is an addiction and doubting that it is. Could we think about better design and involving children in design? Absolutely, yes. You have the expert on this subject in the room. It is all about the defaults and finding ways not to maximise eyeballs, as they charmingly say, so it is not all about attention. Again, it is going to be either regulation or more differentiated business models. Part of me wants to think that this is just a very early stage in a whole new field and there will be more differentiation coming up. If there needs to be regulation, yes, let us regulate with notifications, endless reminders and pop-up reminders to say, occasionally, "Have you have been on too long?" There are ways in which you can set for yourself how long you want to be on before you go and get your homework done. Lots of better ways of managing attention could be designed in, which would be in the interests of the child, rather than in the interests of profit.

Tony Stower: It is an interesting point. You were talking there about what information children should be given and how they should be educated about this. That is absolutely part of the answer here. We at the NSPCC provide help and support both to children and to parents about how to set the controls appropriately and how to agree, as a family, what amount of screen time is responsible and useful, for instance, but that is only part of the problem. If we rely on children to make the right choice for themselves all the time, we can expect that some children will not make the right choice. They are children: they are pushing boundaries; they are testing and all of that.

As a society, we should expect that these services are safe and appropriate for children: every site, app and service. We should not expect children to have to remember what the settings are from what site and that they do not apply here, because there are different rules on the next site—that there is an app that is different here that resets itself every time you log in. We should expect that children, especially younger children, have the highest level of default privacy settings and parental controls. Then, when children and parents understand the impact of those settings, there should be an opportunity to loosen those controls, as children and their needs develop. It is clear that the level of co-ordination and compliance across the industry is very shallow at the moment. While there are pockets of good practice, some sites and apps are better than others, and some services in those sites are better than others. There is no consistency whatsoever, and we would be arguing for the regulator to take a strong approach on that.

Q76 **Lord Gordon of Strathblane:** On the point you were making, it seems to me that having 13 as some sort of minimum age is frankly daft. What we are really looking for is a platform that is suitable for seven year-olds and can be used by them. Would you agree?

Professor Sonia Livingstone: Yes, I would want age-appropriate design and different services for children of different ages.

Tony Stower: The whole concept of age verification at separate ages is unhelpful. We know that parents often defer to these settings. They may well think that, if the site that says it is okay for children at 13, that site is obviously safe. We know that, although the minimum age might be 13 for many sites, there are no special controls for children between the ages of 13 and 18. They may well be exposed to content and behaviours by adults that are totally inappropriate for them. We expect safety for all users; then you may have the capacity to turn off some of the controls.

Professor Sonia Livingstone: It comes back to the point about what the regulator does. If a company claims that its service is appropriate for a certain age group, there has to be some kind of independent verification of that.

Q77 **Baroness Bertin:** Could we bring it back to the education point, digital literacy in particular, and whether you think the Department for Education is as engaged as it should be in the curriculum? This Committee previously recommended that digital literacy should be part of the PSE curriculum. Whether it is going to be remains to be seen. What are your views on that?

Tony Stower: We are awaiting a decision from the DfE on the future of RSE and PSHE in schools in England. We have heard good messages from it, but it is not yet clear quite what the extent of the online safety messages is going to be in those lessons. At the moment, it is very much left to charities, such as the PSHE Association and us, to work together to come up with some of these lesson plans. There is not very much coming out of DfE that is appropriate. We would not want to see simply a lesson here and a lesson there about online safety. We would want to see this as part of schools preparing children for adult society.

Baroness Bertin: From a young age, children learn not to get into a car with a stranger. It is a rather clunky analogy, but we have to try to apply that to the rules of the road of the internet as well.

Professor Sonia Livingstone: I would suggest that it is a bigger challenge than that. I remember the policeman coming to my school when I was little, and we had the afternoon to learn how to cross the road, which parents reinforced. Now, we are trying to understand and help children grasp a very complex system that is changing all the time. With respect, it would be problematic if it were left to charities, which can disseminate and do occasional forms of awareness raising, but education is a process that involves a pedagogy that requires trained teachers.

Baroness Bertin: It has to be placed in the system.

Professor Sonia Livingstone: Yes, absolutely. I am told that, at the moment, digital literacy is approximately one hour in the citizenship curriculum in our secondary schools. The subject association is incredibly under-resourced and pressured. It is not just a matter of saying we want schools to take it on; it should be absolutely clear what is done in PSHE, what is done in citizenship and what is done in the computing classes, which are also required to teach children how the internet works, which is part of what they need to understand.

Baroness Bertin: There needs to be training of the teachers, presumably.

Professor Sonia Livingstone: There needs to be continual training of the teachers because, if a teacher teaches for 40 or 50 years—although people do not usually last that long—it is not going to be what they learned in their initial teacher training. It is a very serious task. The Department for Education should clearly be involved.

Baroness Bertin: Am I hearing from you, then, that the Department for Education needs to double-down on this issue a bit more?

Professor Sonia Livingstone: I do not know what the thinking at the Department for Education is, but I have been at hundreds of meetings about children's internet safety, rights and literacy, and I very rarely see anyone from that department.

Tony Stower: This can only be part of the comprehensive solution. Digital literacy, the new Green Cross Code or whatever can only be a very small part of this. We cannot expect that children, even if they have all the lessons and this is baked into the system, will always make the safest choices for themselves. We need a wider system that respects their needs and their developmental position.

Professor Sonia Livingstone: It must provide a safety net because, however good education is, we know it reaches 20% really well, 70% fairly well and there is 10% it does not really reach. Those are probably the ones who come to the attention of NSPCC.

Tony Stower: That is absolutely right. With any solution, whether parent-based or education-based, there will be children who simply cannot take advantage of it, perhaps because they are being looked after or have chaotic home lives, which we deal with quite regularly. That is why the systems themselves need to be safe from the first moment that a child goes online.

Q78 **Viscount Colville of Culross:** I would like to ask you about data protection and privacy. Do you think the platform should do more to tell children and young people about how their data is being collected, or do GDPR and the Data Protection Act have that covered? Is there enough transparency and privacy built into those two pieces of legislation?

Professor Sonia Livingstone: We are waiting to see; that is the honest answer, because the GDPR and the Data Protection Act are only just coming into force. We have not yet seen what all these child-friendly and child-interpretable terms and conditions will be like. We have all seen, from the endless requests to update our privacy permissions on any service we have used, that we are still in the land of tick-box exercises and user-unfriendly or privacy-unfriendly defaults. You can scroll down and read the terms and conditions, but I know I have been staring puzzled, asking, "Does that mean you are going to collect or not going to collect?" Children will be in a much worse position. It might be that this is what the ICO has in its sights, action will be taken and everyone will start learning much better what good practice looks like, because the companies just do not know what good practice looks like, but it might be that a lot of great hopes are about to be disappointed, in the form of the GDPR.

Tony Stower: There is nothing to disagree with there, Sonia. We simply do not know. It is worth saying that the advent of GDPR brings certain benefits to children, including the right of erasure, which could be a very powerful tool. Children who have uploaded their personal information to social networking sites have the absolute right to have it removed, in almost all circumstances. This is all well and good. If you ask Facebook or Twitter, they will say that you can delete your account and that is that, but it is not going to be that simple for children in reality. If you delete your account, it may delete the data, but it also cuts you off from your friends. Children are not going to make those kinds of choices in that way. There needs to be more granularity.

However, we also think there needs to be a much more expansive approach taken to the right of erasure. If you think about photographs that children might upload, particularly what are called self-generated indecent imagery, so nude selfies, the ICO is very clear that personal data, under the GDPR, is data that is about you. If you take Facebook's approach that you can simply delete that data from your own account, that is all well and good, but that photo may well have been shared elsewhere. It may well have been screenshotted, so the metadata has been lost. It may well be going all round your school, or in even less savoury hands. We are clear that a really expansive approach needs to be taken, and Facebook and the other sites need to work closely with ICO and children's groups such as ours to make sure that children can genuinely delete their data and make this a reality.

Professor Sonia Livingstone: That is the safety side, but the privacy side is also that the data has gone to all kinds of third parties that nobody has any idea about. What is the process of getting back all of that data and all the metadata? I do not know. The experts here will know exactly who owns that and the limits of the definition of personal data. Who owns the profile that has been created about you? Who owns the way in which discriminatory decisions might be made about you in the future, because of the collation of data from multiple sources? How we and our children are going to get that back, I cannot imagine.

Q79 **Baroness Kidron:** This is a slightly leading question, because I introduced the age-appropriate design code into the Bill, so I need to put that on the record. Do you think what you have expressed about the design of services goes to the design of data? To your point, we have to do it upstream. Before all that dissemination, we have to consider what is appropriate to take from children.

Professor Sonia Livingstone: Your remit is whether the internet should be regulated generally, not just for children. Some things might be better done for everybody, like control over third-party data and regulation of profiling. Some things are better done particularly for children. I do not know that the GDPR has got the balance right in that regard. It is unclear about profiling children. We might want to say that children particularly should not be profiled. Adults might understand that they should be profiled.

To your point, yes, I absolutely favour particular protections for 13 to 17 year-olds, different from but no less real by comparison with those for zero to 12 year-olds. One of the interesting questions for this Committee is how far control over data should be better guaranteed for everybody. That might be the best way of protecting children in the long run.

Baroness Quin: My question was widening it out from children to the protections for all of us, basically, but you have just alluded to that.

Q80 **Lord Allen of Kensington:** Tony, in your written evidence, you said that 50% of 12 year-olds have a social media account and the minimum age is 13. I would like to explore further what practical policies online platforms should follow on things like age verification, privacy and anonymity. Do you have specific things you would like them to do?

Tony Stower: Absolutely we do. I alluded to the issue about age verification before. I am never quite sure what problem it is trying to solve. Yes, if the technology was there to allow robust age verification at 13, we would know that only 13 year-olds could be on a site. Absent any other protections, it would not be of great benefit to 13 year-olds and, inevitably, there will be children on either side of the boundary who may benefit from being on the other side of it.

There are things that we think the internet companies should do and simply are not doing at the moment. That is why they require regulation, in our view. The first is that they need to be much better at dealing with grooming. We know that sexual grooming happens and is incredibly widespread in the UK. In fact, in the first year of the new offence of sending a sexual message to a child, the police recorded over 3,000 offences in England and Wales. We released that figure this week. These are messages that have been sent across social networks—text messages and things like that. We cannot quite be sure how many children those offences relate to, because some offenders will send messages to many children at a time, but there is simply not enough action by the networks themselves to pick up those kinds of issues before they arise.

We want them to put in place effective algorithms to detect the kinds of behaviours that we know groomers use. They may be sending "friend" requests to children they have no familial connection with or are geographically distant from, or receiving a large number of rejected requests. We know that many groomers use that approach. There is a developing science of techniques around the linguistics that groomers use. Cardiff University in particular is focusing on some of this stuff. The internet companies are great at using linguistics to target advertising; we know that this is something they could do more of to prevent grooming. We want them to be better at liaising with the police service, so that the police can understand more about the techniques they say they are already using.

We think that children should be told and directed to support when they are at risk of grooming. One of the features of grooming is that, too often, children do not realise they are being groomed until it is too late. It is more often discovered than disclosed. We want to make sure that children are directed to services such as Childline, which can offer help and support.

I should say one other thing before we move on: we also think that all under-18s should have safe accounts from the first moment that they go online. Unless an account can be proved to relate to an over-18, the geolocation setting should be at the highest privacy protection. Live streaming should be protected, so that only verified friends can view it. There are various controls that we would like to see for friend requests as well. All these should be set at the highest as a default, with strong educational measures so that children know what they are doing if they are loosening those controls.

Lord Allen of Kensington: It is something we covered in our last report, but are you still getting resistance from the companies and platforms?

Tony Stower: We have been banging on about this for quite some time and some sites are doing very well at this, actually. Some companies engage with us and have made quite a few improvements, but even those sites are coming to it late, after we have had a go at them, and there is no consistency across platforms. We would like to see safety baked in by design, from the first moment that a service is thought of. There is a tendency in the internet world for designers to think that the end users are like them: they are largely adults, who are intelligent and have the capacity to make a careful discrimination between people's bona fides. We are clear that children do not have those skills in all cases, and they need an extra bit of help to protect them.

Professor Sonia Livingstone: I absolutely agree with everything Tony just said. About 10 years ago, the predecessor to the UK Council for Child Internet Safety, which was the Home Office Task Force on Child Protection on the Internet, made a code of conduct that pretty much contained many of the things that we and the child's rights, welfare and wider stakeholder community wanted to see. It wrote that code, which was adopted by the UK Council for Child Internet Safety in 2010 and, as far as I can see, never implemented. It was not implemented for a number of reasons that are deeply regrettable.

One genuine problem is identifying to whom it applies in the first place. Who is this? We can see that we want Facebook and Instagram in there, but do we know about musical.ly and do we have Omegle on our radar? Have we thought about all the others? When the NSPCC, in its Net Aware project, began reviewing the 50 top social network sites that children use, you could not find a person who could name those 50. It is an extraordinarily long tail, with a number of platforms coming in all the time. They all have to be brought into it, because what we know about children is that, if we make some services safe, they will go to the others. That is why an inclusive approach is necessary.

One of the interesting points in the GDPR that we have yet to see working is that regulation, especially interventionist regulation, is meant to be risk-proportionate. That means that all these companies now have to do risk impact assessments, taking into account the likelihood of children, including vulnerable children, being on their services. We do not know how that is going to pan out, but I hope that the ICO makes sure that those assessments are adequate.

Q81 **Baroness Quin:** I will just raise the international dimension, both European and worldwide, to see what you feel or hope might happen in terms of international and European co-operation. Sonia, you have been working on some aspects of the UN Convention on the Rights of the Child, so it would be interesting to have your take on what could happen there. At the end of the last session, we were looking at the effect of the UK leaving the European Union, the possible loss of influence and whether it will make a difference in reality, because we will want to stay as close to its decisions as possible. Your thoughts on both the European and international dimensions would be helpful.

Professor Sonia Livingstone: If it is complex in Britain, it is even more complex when we look first to Europe and then internationally. Even in Europe, we can see regulation pulling in opposite directions. A lot of the difficulties we are having with the way in which companies act are because of the electronic commerce directive, which makes them platforms, not publishers and not responsible. I do not know whether it is feasible, or even desirable, for Britain to move away from the e-commerce directive, but I hear a lot of discussion about how we might make platforms somehow more like publishers, if it can be done politically. If Britain can be part of that push on a larger canvas, it is much more likely to be impactful than if we become a weird space in a weird market, in which I cannot imagine how international companies are going to operate or respond.

On the UN Convention on the Rights of the Child, I and some others wrote a case for general comment for the Children's Commissioner. It is about the Committee on the Rights of the Child's mechanism for ensuring that a particular new issue on the horizon, such as the digital environment, is properly attended to by all the countries that ratified the convention, which was everyone apart from America, sadly and curiously. This matters, given the headquarters of most of the companies that we are talking about. The committee is certainly making very positive signs. If that were to go ahead, it would set out an ideal statement of what could happen.

In a parallel process, I have been advising the Council of Europe, which is about to pass a recommendation with guidelines for its member states on how to translate the UN Convention on the Rights of the Child in terms of the digital landscape. What does it mean for privacy protection, participation and parenting responsibility across the board? These statements are as good as the paper they are written on, in a sense, if they are implemented. They provide a gold standard, a sense of what the to-do list looks like and a statement of what "good" looks like. There is a lot of uncertainty in this space about what "good" could look like, so this is some thoughtful, rights-informed thinking.

As soon as you switch to a rights framework rather than a protection framework, you get the question of harms. That is not to make it less important, but to see how it is part of a bigger picture. This is also about children's participation and positive provision for their benefits and opportunities online. We should be part of it, putting our enthusiasm into it and making it happen. We are not especially doing that at the moment. I do not know that this is a landscape for which we can make a Britain-only set of provisions.

Tony Stower: I wonder if some of my comments might run slightly counter to Sonia's. There is a great deal of international co-operation in this space already. The IWF, which you have heard from, works with many international partners. The WePROTECT Global Alliance is an international group that is attempting to bring together some players here to make the internet better. We at the NSPCC have some concerns about what happens to children after Brexit. I have no idea what is going to follow the e-commerce directive in domestic law. It would be great to hear if you do. Certainly, we do not know what is going to happen after we leave Europol, the European arrest warrant and Eurojust, which helps to co-ordinate some of these investigations. We have expressed concern about that in the past.

We are dealing with global companies, but the UK is a very big market. For several of these companies, the UK is their second-largest market in the world. They have told us at times in the past that you simply cannot have a domestic one-country solution to this. I just do not believe them on that, to be honest.

Lord Gordon of Strathblane: What about China, for example?

Tony Stower: I am not sure that is the example I would choose but, while most of these companies are based in the US, they have subsidiaries within most countries and target advertising very closely, even at the subnational level. It is certainly possible to put in place restrictions there. In different countries that have different language requirements, they have moderation in local languages, usually based in that part of the world, if not in individual countries. We know that global companies have adapted to local regulations for many years. Think about simple things like product safety and electrical plugs. If you buy a toaster in this country, it has a three-pin plug; if you buy one in France, it has a two-pin plug. That is a very simplistic example, but it is quite possible to adapt your business models. It might not fit within current business models, but they are always adaptable.

Look at what has happened in Germany with the recent legislation on hate crime. The German Government have taken a very strong line, which is that companies that host hate content must remove it within 24 hours of being notified and within less time for the worst content. That has not been smooth sailing for them, but we have seen a ramping up of the number of moderators and approaches they have taken. It is eminently possible to do this, if only there is the will.

I should say that the UK is already regarded as an international leader in parts of this space. We talked earlier about age verification for pornography. We know that several jurisdictions around the world are looking to the UK. They want to see it being a success here, so that they can adapt it to their local situation. It is possible to regulate on a UK level. Of course, there will be norms that we need to think about applying internationally, but we should not let the absence of an international framework prevent us moving ahead.

Baroness Quin: Picking up the last point that was made in the previous session, there seemed to be one view that America was going to remain rather distinct from Europe in its way of doing things, its legislation and so on. Another view was that, because of the internationalisation of industry, they are coming closer towards the European model and an international consensus. Do either of you have a view on how America is moving?

Tony Stower: I am afraid I do not have anything to add on that.

Professor Sonia Livingstone: We can see some subtle differences in the ways in which America prioritises parental responsibility and rights, perhaps, over children’s rights. We sometimes see this playing out in the internet space. I hear informally from a number of companies that they would like everyone to agree on the one model. They fear that model of different provision in different markets. We can see that America is much tougher in some ways, but at the moment it is much looser in how it provides for and protects its children.

Q82 **The Chairman:** Maybe it was just on the basis of the questions we have asked, but neither of you has spoken much about the role of parents and parenting. We have used some analogies about the role of parents. My parents taught me how to cross the road and that was reinforced in lessons at school and in television campaigns. My parents primarily told me not to get into a stranger’s car and that was reinforced elsewhere. You have not spoken much about their role. Is that because these issues are too difficult for parents who were not born in the digital age, when their children were, or is it because the quality of parenting is not adequate? Were you in fact referring to parents when you were talking about the need for education and support?

Tony Stower: It is quite a big issue in the limited time that we have. The first point is that parents absolutely are part of the solution to this problem. The NSPCC works with parents to provide them with information. The Net Aware tool that Sonia talked about is primarily aimed at parents, to help them understand what parents and children think about the apps and sites that children use. We have workshops with parents to help them understand some of this stuff as well.

It can be very difficult for parents to keep up with the latest games and apps, because they change all the time. If you look at Omegle or musical.ly, they only arose in the last three or four years. Facebook is old hat to young people now. While parents may not understand the details of how to talk about individual games, apps and sites, they have many adult skills that they can pass on to their children about how to assess people's approaches and how to keep yourself safe generally, which you and I would perhaps take for granted.

We also need to remember that not all parents have those skills and abilities to keep their children safe. It is a well-known trope now that parents face more pressure than they ever have, especially in families where two parents are working. People may just not have the time and not everyone has parents, so we cannot rely on parents to protect their children. These issues are discussed on internet forums and sometimes, late at night, if I want to get myself enraged, I go on and look at them. I take exception when the answer always comes that it is down to bad parenting. We see in our services up and down the country that it is not that. So many children simply do not have parents who are capable or who are even there, who can protect them in this way. That is why we have focused our lobbying and influencing work on the companies instead, to make sure that the services are safe from the first moment that children use them.

Professor Sonia Livingstone: I have spent a lot of the last couple of years interviewing parents. Most parents are absolutely willing and quite keen to engage with this issue. They do not know where to turn and they are getting a lot of advice, much of which is proprietary and competing. It says, "Come and use our service and our solution", but they do not know how to weigh that. A lot of it is wrapped us as educational, but really it is not. A lot of it is wrapped up as protecting privacy, but it may not be. They need somebody to mediate and evaluate the claims that are coming at them.

What they are told is misguided, in a way. A lot of parents tell me about screen time. I do not say it is not an issue, but what the kids are doing on the screen is more important than how many minutes or hours they have been on it. There is a desire for a simple solution. Judging the kinds of interactions your child is having online or the kinds of services there to protect them is a fantastically hard task, and nobody is speaking to parents except those with a particular interest at stake—apart from the children's charities, which cannot be expected to do everything; or maybe they can.

The Chairman: On behalf of the Committee, can I thank our witnesses? We are very dependent on evidence. We like to make serious evidence-based conclusions, and you have given us ample evidence from a very expert perspective today. We would welcome any further evidence that you come across. It is a developing area, as we all know, and our inquiry will take some time, so we would welcome any material that crosses your desk that you think may be of value to the Committee, if you would forward it to the clerk. Similarly, if there is anything you thought we might have talked about today and did not, or anything that you might have said but did not have time to, please do not hesitate to write to us and give us the benefit of your wisdom. Thank you again for taking the time to be with us today.

Dr Ewa Luger and Professor John Naughton – oral evidence (QQ 93-102)

Tuesday 26 June 2018

Watch the meeting

Members present: Lord Gilbert of Panteg (Chairman); Lord Allen of Kensington; Baroness Benjamin; Lord Bishop of Chelmsford; Baroness Chisholm of Owlpen; Viscount Colville of Culross; Lord Goodlad; Lord Gordon of Strathblane; Baroness Kidron; Baroness Quin.

Evidence Session No. 11 Heard in Public Questions 93 - 102

Examination of witnesses

Dr Ewa Luger, Chancellor's Fellow, Digital Arts and Humanities, University of Edinburgh; Professor John Naughton, Senior Research Fellow, Centre for Research in the Arts, Social Sciences and Humanities, University of Cambridge.

Q93 **The Chairman:** I welcome our witnesses to the second evidence session this afternoon in the House of Lords inquiry into regulation of the internet. I remind them that the session will be recorded and broadcast online, and a transcript will be taken.

Our witnesses are tech experts. We are very grateful to you for taking time to be with us today. Would you start by briefly introducing yourselves?

Dr Ewa Luger: I am a chancellor's fellow in digital arts and humanities at the University of Edinburgh in the Centre for Design Informatics. My disciplinary background is political science and, more recently, human-computer interaction, specifically the ethics of intelligence systems. I am a consultant researcher to Microsoft Research on the subject of artificial intelligence and ethics.

Professor John Naughton: I am a senior research fellow in CRASSH, the Centre for Research in the Arts, Social Sciences and Humanities in Cambridge. I am the technology columnist of the *Observer* and a historian of the internet. My background is as a systems engineer, and over the last two decades I have been studying the impact of the internet on society. I recently finished a research project, which Professor David Runciman and I ran at Cambridge, on the implications of digital technology for democracy.

The Chairman: Thank you. Could you start by giving us a brief account, if that is possible, of how the original infrastructure of the internet developed. At the time of its development, and in its early years, what were its values? How does the internet as we know it today differ from the internet as it was invented and the values envisaged when the internet first came into our lives? Who is best placed to start?

Professor John Naughton: Having written a history of it, perhaps I should start.

The Chairman: I think there is a history lesson for us.

Professor John Naughton: Before we start, can I make one point? It is important to distinguish between the internet, which is the underlying technology, and the services that run on it. I have found over a long period of discussion with politicians and others that that distinction escapes many of them. For example, many people think that the worldwide web is the internet; many people used to think that Google was the internet; and there are now probably a billion people in the world who think that Facebook is the internet.

That is important, because in any discussion about regulation we have to distinguish the infrastructure from the services that run on it. Much of the conversation is about what we do about the manifest social harms that some companies and services that run on the network are doing, so it is important to distinguish.

Going back to the history, the network we use today is very old technology; its origins go back to the 1960s, perhaps before. The network we now use, based on the TCP/IP family of protocols, was switched on in January 1983. Design work on it went on for 10 years before that, starting in autumn 1973.

The people designing the network were faced with an acute problem: how do you design something that has a reasonable chance of being future-proof? They approached that problem by having two fundamental axioms. One was that there should be no central ownership or control of what they designed; the second was that they should design a network that was not optimised for anything they knew about at the time. That meant in the end that they designed a network that was, in their words, extremely stupid. It did only one thing; it took in data packets from one of its edges and it did its best, with no guarantees, to deliver them to the destination at the other side.

The implication of that was that they left all the ingenuity to the edges of the network. If someone had an idea that could be realised using data packets and they were smart enough to write the software to do that, the internet would do it for them with no questions asked. There was nobody they had to ask for permission to do that. In other words, although they did not use this term at the time, Vint Cerf and Bob Kahn, the two originators of the idea, produced an architecture for what later came to be called permissionless innovation. That is absolutely critical, because it meant that they designed a system that enabled a huge and absolutely staggering explosion of creativity. In essence, those two axioms enabled us to create a global machine for springing surprises. That is the best description I can think of for the internet as an architecture.

As we know, some of those surprises have been very pleasant. The worldwide web is one; it is more or less the invention of a single person – Tim Berners-Lee. We regard Voice over IP, Skype, Wikipedia and a whole range of things as the great benefits of the network for society, but because it enabled permissionless innovation, and not only good people are ingenious, it turned out that it also enables a lot of rather nasty surprises, which is one of the things we are concentrating on.

I bring that up because the network itself, as I have described it, requires some attention from a regulatory point of view, but it is not the same kind of attention that we need to focus on the companies that have captured and dominated it. The values, as I said, were openness and the sponsoring of creativity, and everything else followed from that.

The Chairman: Dr Luger, what is your perspective?

Dr Ewa Luger: I have nothing to add.

Q94 **Lord Gordon of Strathblane:** I think I know the answer to my question in light of your introductory remarks. Was the development of platforms almost inevitable?

Professor John Naughton: The evolution of platforms was inevitable; the evolution of the platforms that we got was not. The first great platform, the greatest of all, was the worldwide web, which was conceived and implemented as a public good rather than private property.

Lord Gordon of Strathblane: What do you think are the consequences of the way the internet has developed?

Professor John Naughton: If you look at it from a historical point of view, it has followed a pattern for which there is a great deal of historical evidence. Some years ago the American scholar Tim Wu looked at the history of the great communications technologies of the 20th century in the United States: the telephone, broadcast radio, broadcast TV and the movies. He found the same pattern in each case. The technology arrives; it is exciting, chaotic and open, and encourages all kinds of utopian hopes, but it is hard to use at the beginning. Eventually, along comes a charismatic entrepreneur who makes an offer to consumers. Most normal people, by the way, are not early adopters. The only people who are early adopters are masochists like me, because we like the challenge, but normal, sensible people do not; they just want something to work.

At the beginning, none of those technologies just works, but along comes an entrepreneur—at the moment it is always a "he"—who makes a proposition to the consumer: "I'm going to give you something you can use out of the box and you won't have to think about it any more". In the case of the telephone, it was Theodore Vail of the Bell network whose offer to the consumer was, "If you have a Bell telephone, I make you two promises. The first is that when you pick up the phone you'll get a dial tone. The second is that you can talk to anybody else in the continental United States who is on the Bell network". Those were the two propositions he made. The same is true of the movies and other things.

You get to the point where an entrepreneur arrives, makes a proposition and the industry is captured, sometimes with government or regulatory approval, as in the case of AT&T or the Bell network. That happened to all those four technologies in the 20th century. Tim Wu's question was, "Is this going to happen to the internet?" We now know the answer. It has been captured by a number of giant corporations.

Lord Gordon of Strathblane: But it is not one individual; it is a number of corporations.

Professor John Naughton: Yes, it is.

Lord Gordon of Strathblane: Are there advantages in the dominance of some of these platforms, in that there is interoperability and other advantages for users? In other words, is dominance a not wholly bad thing?

Professor John Naughton: This is one of the great arguments. I am not an anti-trust specialist, but having listened to the earlier evidence I can see that there are people in the field of competition law who think a lot about it. The point is that it is two-sided. On the one hand, because of the network effects that are very important for technology, it is very convenient for consumers if there is a dominant search engine, such as Google, because, apart from anything else, it gets so much data from its users that it constantly self-improves, and that is a real benefit.

The argument in relation to dominance and anti-trust is very simple. Our original concept of anti-trust was that, if a company became dominant and abused that dominance by, say, gouging consumers with prices that it could not justify, that was a bad thing. The problem we have with these companies is that they do not charge their users for what they provide; the users are not their customers.

Lord Gordon of Strathblane: They are users of the product.

Professor John Naughton: That is right. The real customers of Google and Facebook are the advertisers. There may be a case for consumer harm when it comes to advertisers, but it is very difficult to use the anti-trust thinking that we have in relation to the corporations, simply because their services are free, and because their services, as far as the users are concerned, are rather good. You could argue, and people do, that to punish Google because it has 95% of the market and charges nothing for its services is punishing excellence. There is a case for that, and that is why it gets complicated very quickly.

Dr Ewa Luger: Users tend to expect interoperability. The idea of a seamless user experience is hard-coded in our expectation as consumers and in the rules we adhere to when we design interfaces. Anything that breaches that is problematic. The models that underpin some of that interoperability, and the models by which data is collected and used, are not expected, seen or understood by users. If they were using a Google service and an ad popped up, the majority of users would not necessarily understand what had triggered that advertisement; they would not know that it was data from their personal emails, for example. We do not have good, robust mental models for how these systems operate.

Q95 **Baroness Kidron:** It is fair to say that the evidence we have had so far is slightly binary. One set of people says that the OTT companies are there to share creativity: "Get closer to your family. We help you find things that you might be interested in". The other side says that it is compulsive, quite mindless and deliberately designed to make you do things that you may not otherwise do. I do not think the word "spooky" came into the evidence, but there are those accusations.

My question is about the design. I would like both of you to talk about the interface of where we are now. Professor Naughton, you said you loved the promise of the first order—Wikipedia, the worldwide web, et cetera—but how does the interface affect what users see, and specifically how does it both create their behaviour and then capture it?

Dr Ewa Luger: A lot of the ways in which we design user interfaces are to minimise mental workload. You do not want a stressful experience when you are interacting with the system. In that instance, the more data gathered about an individual, the more likely you are to reduce their mental workload by giving them exactly what they want, effectively by predicting their behaviours and, therefore, being responsive in the solutions you offer them. That is where we are at the moment in the design of systems.

There is a trend, which I think will be a future trend, towards the minimisation of the manipulation of the user interface. You sit typing at your laptop, but increasingly we are seeing systems where we interact through natural user interfaces or where data about us is being passively collected, such as applications on our phones collecting location data passively. There are new applications at an experimental stage that would collect snippets of your voice to judge things such as your current mental health and link that to your location data to see whether or not you are depressed.

Baroness Kidron: I am now.

Dr Ewa Luger: It is a bit worrisome. We are also seeing a rise in voice interfaces, but I do not know whether they will take off; it seems to peak and then dip. Research that I have conducted in that area shows that users do not understand what is going on when they interact through a voice user interface, simply because their expectations are based on the model of communication between a human and a human and a theory of mind, assuming you know what the other person is going to say and that you have a common frame of reference.

That does not work with a computer, but we have no alternatives. There are no robust mental models or metaphors that we can use to communicate how systems collect data, what they do with it, how it flows and how it is used through interface design. That simply does not exist right now. People are starting to explore it. We see papers coming out from the leading human-computer interaction conferences, but they are certainly not principles applied at industry level, and that is desperately needed.

Professor John Naughton: I take a bleaker view. We have to make a distinction between the companies. There are five, and two of them have a very specific business model, which is very unusual in our history. The name we have for it now is surveillance capitalism; it provides free services in return for the unrestricted right to exploit the personal data and data trails left by users. In some ways, it is better to think of Facebook and Google not as tech companies but as if they were oil companies. They extract data, refine it and then sell it in one way or another. That is the simple way to think about it.

Currently, it seems a very successful business. To make it work, they have to make sure that the supply of data and the data trails provided by the users of their free services continually increase. That is the key bit. How do they do that? It is very simple. They deploy, among other things, much of what is known by applied psychologists—for example, to increase people’s likelihood to go back to something else, and to incentivise users to stay longer on their platform.

A serious degree of addictivity is built into these services, which is why when you talk to people who use them and ask whether they are concerned about how much time they spend on them, you get a funny sort of shrug. Somebody goes on to Facebook to check a picture from a family member and an hour later they wonder why they are still there. They are still there, because it is beautiful software that is very cleverly designed. In a way, the core of this is the business model of surveillance capitalism. That is the key, and, if we want leverage on that particular kind of corporation, that is where we have to look.

That is why competition law is important, because that may be the interesting place.

As to addictivity and the rest of it, there are other things—for example, the fact that there is huge peer pressure to use the services. In some cases, the social pressure to be on those services is pretty compelling for young people, teenagers in particular. Although you can say to somebody, "You don't have to do any of this. Nobody is forcing you to use Facebook or Google", they will say, "I don't have any options socially".

Q96 **Baroness Kidron:** I should declare that I wrote a report about persuasive design, which was published last week. I put that on the record.

I want to move to the question of children and vulnerable adults. Going back to your historical description, in a way many of the people who designed it say that it was a democratising technology; there were going to be no gatekeepers and all users would be equal. I want to ask about the "all users would be equal" piece of it, because children spend huge parts of their childhood in an environment that was not designed for, nor did it anticipate, their presence, and in which as a concept childhood largely does not exist. I think you can extrapolate from that to some other users. Could I have your opinion on whether the design of services adequately meets the needs of different user groups, particularly the vulnerable?

Dr Ewa Luger: Absolutely not. There are a number of issues. Most services are designed by a particular demographic that does not represent humanity as a whole; it does not represent me. That is a massive problem.

Another thing, which I have been concerned about in my research, is that we have run roughshod over the notion of consent and what it is to consent to the use of your data. I know people push back on the term "your data", but the traces of my existence made manifest through these systems, because of the way they are architected, are not the same as a tangible block that belongs to me or someone else and is actually a reflection of my beliefs and values.

We know that the consent model—the tick and click terms and conditions model—is broken and does not work. People spend less than 30 seconds reading those kinds of documents; fewer than 1% pause to read the small print of end-user licence agreements. There has been research to show that we are trained to accept. When we are presented with a tick-box option, in comparison with any other option, we tick it much faster. Everything about the way consent is manifest on the internet is problematic.

Add to that the idea that consent has to be voluntary, competent, informed and comprehending, and you can see immediately that there is an issue, because what you are describing is competence. A child is not yet able to give consent in any contextual way, so even before we get to the fact that the mechanism is faulty we are putting children in a position where they are agreeing to things they simply cannot understand.

It is not just children. Most people do not understand the implications or harms that can arise from sharing data with particular types of platforms. Most experts would struggle to give you a fair prediction of what will actually happen in the long term.

Professor John Naughton: As regards the history, I would describe myself as a recovering utopian. I am an engineer and I thought we had really cracked it. We had created a wonderful network that would do things that were impossible before, and so on. What I omitted to notice was that all technologies are socially constructed.

This technology was invented essentially by a very select group of males, broadly speaking, working primarily in elite research institutes in the United States, although some of them were in University College London. They knew one another. The network they designed was one that conceived of its users, first, as equals, and, secondly, as people who could be trusted. For example, at the time of the design of the SMTP internet protocol, which determines how email servers work, nobody thought to build in authentication, so a mail server did not check that the mail coming in was in fact coming from the person who purported to be sending it. That is why we have spam. We had a hole designed into the network because of its social construction. Nobody in the 1980s worried about stuff like that. You knew who the person was or you knew where they were coming from.

To go back to Dr Luger's point, we see that now in the services that run on the network. The demographic of the people who work in these companies is fantastically skewed. It is amazingly male and amazingly white or Asian; it is definitely not black. Sometimes you get absurd outcomes—for example, somebody developing a healthcare app that omits to notice that women have menstrual cycles. Demographics really matter in these areas. This is a very skewed demographic in a strange part of the United States.

Q97 **Baroness Chisholm of Owlpen:** This may be like asking, "How long is a piece of string?", but can I ask both of you to look ahead? What do you feel will probably be the biggest changes, and what are your concerns about the internet and all the enabled technologies in the next five to 10 years?

Professor John Naughton: The answer depends partly on whether or not democratic societies decide that they need to do something about these companies. I have a provocative proposition, which is that the only regimes that will be able to control these outfits are authoritarian. The Chinese Government have no problem at all with this stuff. The problem for democracies, apart from the rule of law and all kinds of other stuff, is that it is more complicated. The future depends on whether or not democratic Governments and legislatures summon up the political will to address some of the harms that come from this kind of dominance. If they do not, my feeling is that the future looks pretty bleak, simply because the business model of surveillance capitalism requires that surveillance becomes more and more intrusive.

You may have noticed, and it is no accident, that all the big companies are desperate to have a listening device in your house. The reason is because up to now what happens inside your home is, broadly speaking, rather opaque to them, and they want to make sure that it is not because they need a constant supply of data. Apart from human beings deciding they have had enough, I cannot see an obvious end to that at the moment. If we do not have regulation, we will have real trouble further down the line.

The Chairman: Do you think that in the tech companies the discussion about listening devices you have just described takes place in those terms?

Dr Ewa Luger: No.

Professor John Naughton: Dr Luger is more knowledgeable than I am.

Dr Ewa Luger: I have never heard it discussed in those terms in my experience. The values that exist in tech companies are not necessarily the same values that exist outside them. There tends to be a much narrower product focus. There might be talk about efficiency or creating better and more competitive products. As far as I know, nobody ever says, "We're going to put something in your home that monitors your behaviour".

The Chairman: Do you agree, Professor?

Professor John Naughton: I do, and it is very significant. For example, after the recent Cambridge Analytica scandal, the CEO of Facebook was eventually hauled before the United States Congress. You will have observed that he has declined to be hauled before this body, but never mind. The strange thing is that, if you analyse the transcript of those two sessions, the business model of the company is never mentioned—never. It is like the old saying that nobody would ever eat a sausage if they saw how it was made. It is interesting that many parents who work in the tech industry are very careful about how much they allow their children to use devices.

Baroness Chisholm of Owlpen: Education is paramount.

Dr Ewa Luger: Education of computer scientists is paramount.

Baroness Chisholm of Owlpen: No, education for us. There is no point trying to educate them. I was thinking more of the general public.

Dr Ewa Luger: People are talking about issues such as data literacy and algorithmic literacy, so those things are important. I did not mean to make a flippant point. I believe that we should educate computer scientists in ethics. That does not exist currently.

Professor John Naughton: If you were to take a longer view, the great cultural critic Neil Postman wrote a book in the 1980s entitled *The Disappearance of Childhood*, in which he argued that our concept of childhood is socially determined, largely by the dominant communication medium of the age. He said that was why you never see children in Brueghel paintings; you see only small adults. That was because in the Middle Ages a child became an adult when they achieved competence in the dominant communication technology of the era, which of course was speech. That was why the Catholic Church, from the Middle Ages onwards, set the age of reason at seven.

Postman's argument was that, when print came along, the time it took to get to communicative competence was longer, which was why the age became 12, and we had the beginnings of mass education. He went on to argue, mischievously, that with the dominance of television the age of adulthood went down to three, because you never saw a remedial class in television viewing. The big question for us is: what is this dominant communication technology now doing to childhood? I do not have an answer, but it is an interesting question.

The Chairman: We ought to stick to the ethics of business models, if we may.

Q98 **Lord Bishop of Chelmsford:** Quite a lot of the written and oral evidence that we have received from other witnesses has pointed in the direction of what is known as ethical by design. Dr Luger, this is an area to which you have given particular thought. I would be grateful to hear from both of you what you think is meant by that term, and what principles might be adopted to ensure some sort of ethical by design standard.

Dr Ewa Luger: Ethical by design is one of the terms that has been recently coined. There is no hard and fast definition, but if one were to define it, the most common understanding is that it is the consideration of human values and ethical principles from inception to completion of the design of the technology, from the ideation stage to the point it hits the market. I would argue that we need to extend the context within which it is deployed.

There are four ethical principles that one might adhere to in any context: beneficence—always do good—and non-maleficence, never do bad; autonomy; freedom to act; and justice and fairness. Those things are critical and a lot of them are violated to some extent by the kinds of systems we are discussing.

If we were to drill down a bit to create specific principles, one of them would need to be openness by companies as to how personal data is collected, stored and used, which would include activity tracking and behaviour tracking. There should be an emphasis upon intelligibility or legibility, depending on how you wish to frame it—enough information about how a system operates that a user can meaningfully interact with it. Currently, we do not have that in the kind of systems that are emerging. Next, there is opt-in as default and easy revocation.

Some of those principles are now enshrined in the EU's GDPR, but they have not yet made it into the design of interfaces. How does one do that without, for example, breaching user experience? All those ethical principles have to be offset against developing good user experience, or nobody will use the technology.

Another principle would be enhancing voluntarism. Do people have a genuine choice in using a system? Are there other systems they might use if they choose not to share aspects of their data? Does the system still operate in the same way?

Purpose limitation is also a legal principle, and it is incredibly important. Should the data be used beyond the purposes outlined when the technology was sold or adopted by the user? I would say they should not and the law says they should not, but in reality we see it happening all the time. A really nice mechanism for this in data protection regulation is the idea of the motivated intruder test. Could a motivated intruder re-identify the dataset? Something similar in an ethical context would be pretty important. If you change the purposes, does it become an issue? Minimisation of discrimination is another one that speaks directly to the justice aspect.

In failure handling, how do we deal with transparency and reporting? When a system fails, there is something about interface design that suggests that the computer is always right, but in reality we know that some algorithms are not accurate all the time. Some of that needs to be exposed so that users understand what they are interacting with. In the long term, it is through such interactions that you get a sense of how to engage with the system. Part of it is through good design and part of it is through testing and using a system.

Another aspect is the reproducibility and re-performability of algorithms. Can an algorithm create the same function or output more than once? This is much more complex in the emerging classes of algorithms, such as deep neural networks, but as I understand it it is still possible at some level. We should work hard for that principle.

Finally, we come to provenance. I am surprised that we do not do more instrumentation of record keeping—logging inputs and outputs, and the effects on people through the course of the technology.

Professor John Naughton: This is not my field. I agree with what Dr Luger says in that area.

Ethics also apply at the corporate culture level. Until quite recently, in the technology industry at any rate, ethics were treated like statements about motherhood and apple pie—in other words, as vague bromides. As it slowly dawned on the industry that there might be serious trouble coming, it has started to boost its concerns with ethics. Some of them are quite preposterous in the sense that they are simply public relations stunts. In some cases, there is evidence that a few companies are starting to take this very seriously. The classic one is DeepMind, the Google-owned British artificial intelligence company. I think it is taking ethics seriously.

Having honest business models would be a start. I do not mind paying for, say, Facebook. I am quite happy to pay for it, but I do not want to give it my data. I would like to have that option, in which case we might get to a better place quickly.

The final thing is responsibility. It is absolutely the case that, however critical one is of those who lead some of these companies, broadly speaking they are not evil-intentioned people. In fact, part of their problem is that they believe they are good; they feel that they are transparently good and therefore that they could not be doing evil, but if they operate businesses that produce what look to us like socially damaging consequences, they need to accept responsibility for them.

Lord Bishop of Chelmsford: I was interested in your oil-company analogy. It was a fascinating way of thinking about the companies. Did they set out to be oil companies or did they just discover at some point, "Oh, look, we've got this data and there's money to be made here"?

Professor John Naughton: In the case of the more prominent companies, they did not have any idea what they were going to do when they started. For a long time, both Google founders and the Facebook founder expressed opinions about advertising that suggested it was pretty awful and they would have nothing to do with it. In the end, they discovered that the only way to fund what they wanted to do was to become advertising companies, and they did so.

It is not that their intentions were not good; it is just that they were naive. For example, in the case of Facebook they built an amazing machine for enabling advertisers to target people with messages. It is a terrific machine, and if you go in as an advertiser you really see its quality. It did not seem to have occurred to them that it is not just advertisers who want to target people; it is people like Steve Bannon and other actors. There is a naivety about human nature, which is strange.

Q99 **Lord Bishop of Chelmsford:** That leads me to a supplementary question. It is about ethical by design in particular, but it may cover other things. What role do you think should be played by committees such as ours, government, academia and private organisations in the development of ethical standards? What do you want to say to us, which we might say in the report we are preparing, about ethical standards that could realistically be designed into these systems?

Dr Ewa Luger: The first point to note picks up something that Professor Naughton mentioned, which is the culture of the tech industry and the fact that people do not set out to do harm, but they do not know what the alternative is. Responsible innovation is not embedded in the teaching of computer science, machine learning or AI. There is now a bit more in robotics, but it tends to be mildly flippant, looking at what happens if robots become sentient. I am not saying that those questions are unimportant; they might be at some point, but that is getting ahead.

Changing the culture requires investment at HE level, not simply once the cat is out of the bag and everybody is happily working in a corporation. There is no real incentive for tech designers who are competitive against each other and the wider world to consider ethics unless it is forced upon them. Certainly it is something academia could think about, not simply coming out with a critique of the issues or saying, "There's bias in this algorithm". Those things are important, but we also need to consider that we are producing a raft of people who are incapable of doing anything else, so how do we change that?

It is a matter of embedding ethics in teaching, and developing solutions. There are all kinds of work on that. The United States is dominant, with the work of the fairness, awareness and transparency agenda—the FAT people—and the AI Now Institute and Data & Society. They are already starting to look at these kinds of things. We need plug and play solutions for industry. If we have solutions that we know work to minimise bias, industry will use them, but the expectation that solutions will come internally from those organisations is probably not one that will happily produce any results.

As to government, one of the things that we still do not understand is the long-term harm from data-driven systems. We can speculate, and we can identify when bias occurs, but we do not actually know what automation will mean—for example, minimisation of the workforce and that kind of thing. We do not really know the long-term implications. There are no long-term studies of such things. I suggest we start to conduct long-term studies to look at where algorithms are deployed in areas such as public health, social security and credit scoring, where the negative impacts might be massive.

Q100 **Viscount Colville of Culross:** I would like to ask about the disadvantages of using algorithms online. Professor Naughton, you have talked about the embedded bias of language that may not be picked up by machine learning. You have also talked about the lack of context. Could you explain some of your concerns about algorithms? Is it possible to design an unbiased algorithm?

Professor John Naughton: That question is of the same order of magnitude as whether it is possible to design an unbiased human. We are talking about specific kinds of algorithms, which are machine-learning algorithms. Machine-learning algorithms are basically programs that can convert vast amounts of data into patterns that can be observed or predictions that can be made. What we already know without controversy is that the old rule about garbage in, garbage out applies. Most datasets are not clean; they are coloured in one way or another with all kinds of unconscious and other biases. In those circumstances, there has to be much greater awareness of that. Awareness in the machine-learning community is now pretty widespread. It is very impressive compared with what it was like, say, five years ago.

The problem then arises with the wider community of people who are dazzled by this technology, by which I mean government Ministers, among others, corporate executives and so on. They know nothing about the technology, but they are dazzled by it. We always have to be prepared to apply the standard levels of human scepticism that we should apply to anything. There was a period when that was not happening.

The most spectacular case was when Google revealed that its analysis of queries about flu enabled it to predict flu outbreaks two weeks ahead of the Center for Disease Control and Prevention in Atlanta. This was claimed as a fantastic advantage of big data. It then turned out that Google knew nothing about flu; it was just that its machine-learning algorithms had picked up a pattern. Then there was another kind of flu and it did not work, but that did not stop people extolling the fact that machine learning was the next big thing.

The industry is trying to find ways of dealing with that. One of them is that if you want to do machine learning, on the one hand you have the machine learning doing its stuff; on the other hand, you have another kind of AI, which is effectively a sceptical AI, questioning it. You have a kind of antagonistic approach. There may be technical solutions to some of this, but in the end the problem is that there are always some kinds of biases somewhere in datasets. That is why one has to be very sceptical about using them in an unmediated way as guides to policy or decision-making.

For example, the United States for some years has been using machine learning with considerable and, some would say, impressive success in carrying out analysis to identify targets for drone strikes. That is real life and death stuff, but it has held back from the idea that the algorithm, having identified the target, can then institute the strike. That is the only model we have for the foreseeable future, and if we shift from that we will be in deep trouble.

Viscount Colville of Culross: With that scepticism in mind, should we not allow algorithms to make decisions that affect humans?

Professor John Naughton: At the present stage, no algorithm should be allowed to make a decision that affects the life chances of somebody else, without human oversight or a body that can be held responsible for that decision.

Viscount Colville of Culross: What about much smaller decisions?

Professor John Naughton: I would have to go back to Dr Luger. There are all kinds of areas where low-level decisions are rather helpful. For example, I can ask Google Maps to tell me the best way to get from the Palace of Westminster to King’s Cross. It will do that for me and I will follow it through. There is a level at which it seems unproblematic, but there is a level further up about whether your kid gets into a school, or you get a loan or you get parole. Some systems now do that. In that case, I cannot see any justification for having machines make those decisions.

Dr Ewa Luger: To some extent, there are distinctions to be made about algorithms of the type we are talking about. It comes down to algorithmic capacity, which we have heard about, and the algorithm being the black box. There are three broad reasons for that: one is that somebody looking at it does not have sufficient technical literacy; another is that it would take a trained expert to pull apart the algorithm and work out what it was doing; and the final one is that some algorithms are being developed where even a trained expert could not tell you how it reaches its judgment. For that latter class of algorithms, absolutely not. We do not know enough about that yet to deploy it in sensitive contexts.

As Professor Naughton noted, it depends on the context. If it is Google Maps getting you from A to B, it is fine, but deciding whether somebody should get some kind of health intervention is an entirely different proposition, so these things matter. There is a recent example. Durham police are using an algorithm designed at Cambridge called the HART algorithm. It was intended to predict whether a criminal is a high or low risk.

An academic from another institution did an analysis and suggested they ought to remove some of the predictors, such as location and sociodemographic data, because they might result in a prejudiced view of crime and who was involved. Some crimes are more likely to occur in certain types of places, so the algorithm was prejudiced. That is a nice example of where people are working to minimise bias.

The issue with that algorithm is that it is better at predicting things, which humans are not very good at. There are some things on which algorithms could give us much better judgments. It could save money and create better decisions in the health domain. Lots of algorithms are being used there to help identify whether, for example, multiple sclerosis has moved from one stage to the next.

There are some contexts where it is fine, but you absolutely need human oversight at this point in time. It comes down to whether the algorithm is explainable. If it is a class of algorithm that somebody who is technically literate could understand and an expert could pull apart and tell you how it reaches that judgment, that is one thing. If not, I would warn against it.

Q101 **Baroness Benjamin:** How can we effectively ensure that algorithms are accountable or transparent? Do you think a code of conduct for algorithmic design would help companies to act morally and with integrity and trust, and for that to be embedded in their DNA? Do you think that type of code would do anything to improve accountability?

Dr Ewa Luger: It depends on how the code is enforced or reinforced. There are codes of conduct for lots of main bodies. The Association for Computing Machinery, for example, has a code of conduct and, for engineers, the IEEE has a code of conduct for ethics, but I do not see any real difference in ethical practice. It is important to have codes; we absolutely should, but there needs to be some way that is manifest in the products that are designed, rather than people just agreeing to things that are a little like greenwashing or, in this case, ethic-washing. That is a concern.

There are some developments in the area of explainable artificial intelligence, which is called XAI in the States. Some of the things people are pushing for us to be able to do with algorithms are the answers to a number of questions. Why did it do that? Why did that function occur? Why did it do that and not something else? When has it succeeded and when has it failed? When can the user trust it?

That is about the proportion of accuracy. Is it 80% or 100% accurate, because in the context that absolutely matters? How do I correct an error? DARPA believes that, if you have algorithms that can respond to those questions, you are broadly in the right ballpark.

Professor John Naughton: Codes of practice have a long history and we have had varied experience with them. In general, they are a good thing because they represent a set of aspirations that we would like an organisation or group of workers to adhere to. They are a necessary but not a sufficient condition. I write a newspaper column, so at one level I could be classed as a journalist. Many of you in this House know that the British journalistic industry has various codes of conduct. I invite you to speculate on how effective they have been in relation to tabloid newspapers, for example. Even though the code is there, it does not seem to bite.

Baroness Benjamin: Why?

Professor John Naughton: I do not know. In part, it may be because it is not enforceable in law. That may be the problem, or maybe it is because in a competitive environment ignoring a code may give you a competitive advantage. I am afraid that could be true in this industry, too. Codes are a good thing, because they represent our aspirations, but they are not enough.

The Chairman: There has to be enforcement.

Professor John Naughton: It is code plus enforcement, and, if the code works, you hope you will never have to enforce it.

Baroness Benjamin: What should be the consequences if you do not follow the code?

Professor John Naughton: It depends on the context. It would be very interesting to think of sending the editor of a British tabloid to jail, and what Mr Putin would do with that. There has to be some kind of proportionality, and that is not easy; it varies from context to context.

The Chairman: Proportionality is at the heart of all regulation, is it not?

Professor John Naughton: I am afraid it is, and it is hard.

Q102 **Baroness Kidron:** I am mindful of the hour. I have an enormous question. You might like to answer some of it in writing, retrospectively. One thing that keeps coming up is verification, specifically age verification, and anonymity as a concept online, and the pros and cons of that. There has been a lot of evidence about what privacy should look like. By that, I mean default privacy settings. What policy should there be with regard to anonymity, default privacy and age verification? What are the technical challenges? I understand that all three of those things are quite huge, so feel free to say the top line and then, with the Chairman’s permission, perhaps you could write to us about the detail.

Dr Ewa Luger: There is really only one part that I can comment on based on my research, and that is privacy. We have a large problem, in that our notions of privacy alter almost daily. What people expect and what they are prepared to accept shift in accordance with the systems they use, and that is problematic.

A number of the surveys that have been conducted show that people are concerned about their privacy, but then we see the behaviour-intention gap; they will merrily share any and all data to get the shiny thing at the end of the road. The systems are designed to hit the reward centres of our brains, so that is fairly unsurprising. The whole concept needs to be broken down to some extent; it comes down to what is good for people versus their expectations, and they are not necessarily the same thing. I suppose we could get into a kind of paternalistic role.

Baroness Kidron: Can I push you a bit on that? Their expectations in the current context may be out of kilter with their expectations in any other context, in that they are designed in.

Dr Ewa Luger: Absolutely. I often hear the phrase "Privacy is dead". I apologise in advance for giving a terrible example. We say that and mean it, broadly and socially, but everybody shuts the toilet door and gets dressed and undressed in private. We have expectations of privacy; it is just that when we talk about it our default idea is, "If I've got nothing to fear, I've nothing to hide", but we all know that if there is a context shift, that becomes untrue. The political climate changes, or suddenly some aspect of your character becomes linked to terrorism, and it becomes problematic for you as an individual, because the monetisation model relies on our being profiled and those profiles being sold. Privacy is important because it protects us, but online it is definitely a different model from our social model.

Professor John Naughton: I agree. Privacy is one of those strange contested concepts; it is ambiguous and it is very hard to get a grip on it. One simple way of trying to clarify it a bit relates to the deal you strike with an internet company by clicking "Accept" on its end-user licence agreement. In those circumstances, if you are a user of web mail, particularly Google's Gmail, you make a contract that says, "Google, you can read my mail", so in that sense you are handing over your privacy. That is fine; you make that decision. You and Google are treating privacy as if it were a private good that you can transact in return for services. That is fine for a while. Then you send a message to somebody who does not approve of that and has definitely not signed up to any of it. Replying to your Gmail account, that person emails you. Suddenly, you have compromised their privacy. The point is that privacy is in some ways both a very private thing and a social thing; it is almost an environmental good in many cases. The technology has blurred all of that and made it very, very difficult.

On verification, were you thinking of age verification?

Baroness Kidron: I was in this specific case, because we have laws coming in that require it. It is a slightly difficult area, because the law went ahead of the technology.

Professor John Naughton: It is difficult. The key thing about it, which is worrying, is that in general one should not enact laws that one is not going to enforce, because you undermine the law, as well as everything else. That is really tricky. There are some very worrying developments—for example, the increasing use of tablets and smartphones as a way of amusing very small children. That is really worrying. There is some evidence about what babies need, and it is not a screen; it is a human face. I think that in some authoritarian societies it will become a crime to let your toddler use a smartphone. In our societies, we will not do that. I am afraid you have opened up a huge can of worms and I have no obvious answers.

The Chairman: In that case, we will draw the session to a close. It has been fascinating for us. We noted your warning at the beginning about the breadth of the subject and loose use of the word "internet", and we understand the point you are making. This is a broad inquiry, which will take a long time. I think you have noted our focus on the business models, not just on immediate harms and abuses. Your evidence in that regard has been very helpful and interesting.

I thank both of you for taking the time to be with us today. Please feel free to write to us if you want to elaborate on anything. If some interesting reading crosses your desks over the next months that might be of interest to the Committee, please send it to our clerk. Thank you for being with us today.

Dr Orla Lynskey, Professor Pinar Akman and Dr Nicolo Zingales – oral evidence (QQ 83-92)

Transcript to be found under Professor Pinar Akman

McEvedys Solicitors & Attorneys Ltd – written evidence (IRN0065)

Please accept our submission below. In summary, we do not believe that regulation is currently necessary. We do have concerns about pressures being applied to ISPs to regulate speech in return for immunity and based on soft law, at best, and the impact on freedom of expression. We also believe the UK fails to provide an effective remedy in many cases given our very serious access to justice issues, and suggest these need very careful thought, not knee-jerk reactions or headline-making initiatives.

1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

a. Is there a need to introduce a new regulatory framework for the internet? Is it desirable or possible?

(i) No. There is no present need. See below.

(ii) It is possible with some limits. These tend to be territorial and/or jurisdictional. There is still no comprehensive international treaty for enforcement of foreign judgments[890] and while this has not caused serious issues to date, this is in part as many US companies have decided to voluntarily comply with UK court orders or pre-action demands. However, there are some serious issues that will need to be addressed. Sooner or later, we will need to look at those who are targeting the UK while deliberately avoiding our laws and jurisdiction. Some US platforms that host reviews for example are avoiding UK libel laws and fighting even Norwich (disclosure) orders very effectively on First Amendment grounds for John Doe defendants. This plus the US libel shields (the State and Federal Libel shields, including the SPEECH ACT Law 111-223, 124 Stat. 2480, 28 USC 4101 and protection domestically without takedown under the §230 of the Communications Decency Act 1996) mean that these parties are publishing here with impunity and have an advantage over other speakers. Sooner or later we will have to look at blocking these people –perhaps on a strikes basis. What this means in practice is that the ordinary person can only seek relief takedown from Google (or other search engine) or other intermediary and while this may provide some relief under the new personal data tool, companies will not get takedown. See further below.

There are no easy answers here. We can look at the example of commercial international disputes more generally and see that the New York Convention and its near ubiquitous adoption led to the selection of international arbitration as the main choice for cross-border disputes. It has the advantage of avoiding local state courts and judges which may prefer a domestic party plus internationalised procedural rules and norms. In some ways, having a new chapter of the Convention to deal with cross-border internet related disputes might be a way forward but there are issues and the New York Convention allows challenges to awards on grounds of public policy –which is

[890] There is the Hague Convention on Choice of Court Agreements but this is limited in scope to respecting jurisdiction clauses and so party autonomy on jurisdiction selection in commercial contexts.

circular in that it will take us back to local speech norms or laws. There is a need for international co-ordination and a rule-making forum. Many states are signatories to the UNDHR and there is a level of harmonisation at a Human Rights law level on art. 10 ECHR and its parent, art. 19, with margins of appreciation for signatory states. It should be possible to distil some level of basic rule harmonisation into a treaty. See further below.

(iii) Is it desirable?

No. On the whole, things have worked in practice reasonably well so far. However, this has in part been due to a desire by the big players to be seen as good actors and avoid regulatory attention and sanction. This cannot be counted on indefinitely and we are also arguably now seeing smaller players now who are more prepared to game the rules. See above and further below. There was a wise recognition early on by the UK and US courts and legislatures that nascent technologies and business models should not be regulated into an early demise or quashed. One learned US judge said that after 100 years we should start to think about regulating the internet. There is often a rush to it, but good laws evolve over time and are first tested in the market. English commercial law, for example, has been honed over centuries of trade usage. We can look back and see that without the e-commerce immunities for notice and takedown, the early intermediaries would have been sued out of existence very early on.

b. *In your view, should we encourage self-regulation or employ more direct means such as co-regulation or direct (command and control) regulation?*

The UK's approach from the start -the same rules online as offline –with light touch regulation has worked well and facilitated London as a home to tech, with many industry leaders based here. This also reflects international norms and the UN Human Rights Council affirmed in Resolution 32/13 that "rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice."[891] Good laws are technology and actor neutral and focus on behaviours and not actors, so the first question should remain what happens offline? The UK has laws dealing with intellectual property, revenge porn, privacy and data, harassment (criminal and civil), obscene publications, malicious publications and communications. We also have the Public Order Act (Incitement to Racial Hatred), the Race Relations Act and the Racial and Religious Hatred Act, the Terrorism Act, the Sexual Offences Act and the Protection of Children Act and laws governing advertising and commercial communications, etc etc. Most of these are technology neutral and so, in short, we believe the law is currently adequate and there is no pressing or obvious need for additional legislation. The current approach works well when dealing with regulated speakers, print or broadcast media – where there are co-regulatory and self-regulatory systems which include complaints procedures or arbitration or other means of effective remedy.

Where there is a real issue is how to provide a low-cost remedy/self-help measure more generally against other businesses and unregulated speakers. At present these can only be advanced as data issues to the ICO as there is no other authority in town. Access to specialist lawyers and/or the courts or litigation process is not

[891] See UN Human Rights Council 'Resolution 32/13 on the Promotion, Protection and Enjoyment of Human Rights on the Internet' (18 July 2016) A/HRC/RES/32/13, para 1.

affordable/possible for so many (arguably a violation of the state's art.6 obligations). So if a well-founded takedown notice is given and ignored, the only option is the courts. Ofcom/DCMS probably need to facilitate the establishment of an arbitration procedure for removals on other grounds –this would be self or co-regulatory.[892] This could be based on the domain name dispute resolution procedure for the UDRP (Uniform Dispute Resolution Policy) as administered online by WIPO and CAC and the Forum –all of whom offer paperless and software facilitated platform procedures. This is one of the internet's real success stories. Online justice at its best. It is cheap and fast yet the panellists or arbitrators are all independent experts. It is an excellent model. In the interests of disclosure, I note that the writer is a panellist for CAC and other panels. The public need something like this dealing with removals on various legal grounds where there is currently no effective remedy. This would be preferable to leaving the ISPs to do it –particularly as they are incentivised to protect themselves and obtain an immunity/safe harbour defence by removal.

Those grounds however should be found in or extrapolated from existing law. There are obvious issues and problems with restricting speech based on anything less than hard law, see the art.10 jurisprudence on soft law.[893] There are problems with introducing new restrictions that need definition over time. Existing law has already been interpreted and has known contours. Furthermore –the law already has what is needed.

There are also issues if interpretation and enforcement is left to private interested actors entirely. See the recent decision in *NT 1 & NT 2 v Google LLC* [2018] EWHC 799 (QB) demonstrates this. That decision, was about the very important societal principle of rehabilitation through the *spent conviction*--the ability to serve your time and move on to a second chance under the Rehabilitation of Offenders Act (ROOA). In that decision, the judge decided that only one of the offenders deserved a second chance as only he was remorseful and there was no obvious risk to the public as he was no longer in business and so dealing with the public. The second offender was denied his second chance as he showed a lack of remorse (in the view of the judge) and was still offering services to the public –who had an interest in knowing his criminal past. That denial means he will never be allowed to move on and any search of his name will forever bring up his past—like a permanent tattoo on his name. This decision was about the Right to be Forgotten (RTBF) where the first decisions are taken by the search engine. Recourse may then be had to the ICO and finally, as happened here by the court. Frankly, in our view this decision makes very bad law. It may have some justification (spent convictions may be mentioned if there is a public interest under the ROOA) but how is Google or any other search engine going to assess remorsefulness or judge whether an offender is worthy of moving on? It has an interest in traffic and is not independent. The decision is a licence to refuse the RTBF to any party dealing with the public –which will include tradesmen. Many many people will be denied their second

[892] Ofcom regulates TV and while we don't want the internet regulated under the same codes, Ofcom is the backstop internet regulator under the Communications Act yet does nothing and offers no more general remedy. Note that Mr. Justice Leveson in his Report on the Regulation of the Media was also happy that Ofcom should be the final regulator for the print media if it had failed to join a recognized standards body within a year of being required to do so (as it was they set up and joined IPSO instead which refused to apply for recognition in contrast to Impress).

[893] And see *Malone* v United Kingdom App.8691/79 the court stressed that the law must indicate the scope of a discretion of the executive and the manner of its exercise with sufficient clarity to give the individual protection against arbitrary interference. English law was so obscure and subject to such differing interpretations particularly as to the dividing line between the conduct covered by rules and that by discretion that it lacked the minimum degree of legal protection required to qualify as law.

chance by Google on this basis. We believe this is wrong. There are already many serious challenges for offenders who must re-enter society and support themselves and their families and that was what led to the passing of the ROOA in the first place. In a similar vein, from experience in practice, while the law recognizes that companies have valuable reputation protected by the law of defamation, see per *Jameel v Dow Jones & Co. Inc.* [2005] QB 946 and the Defamation Act 2013, in our experience, Google will not grant a RTBF to a company as it is a personal data right for individuals. There are also issues as to the scope of any relief even where granted.[894]

We examine further below but note here the fact that ISPs are incentivised in their own interests to remove content in order to benefit from defences and the only recourse is to the courts which is not an option for many.

In summary, there are many issues with leaving the matter wholly to the private sector where they get to mark their own homework and/or are self-interested and we believe that the UK state/government should offer an effective remedy to online rights and that the lack of such a remedy is the real issue. We propose an arbitration procedure based on the UDRP model as offered by WIPO and CAC perhaps via existing arbitral institutions but funded and supported by the state and perhaps facilitated by DCMS/Ofcom. This accords with the obligation of the UK under the ECHR to provide an effective remedy under art. 13 to persons whose convention protected rights and freedoms have been violated. The corresponding provision in the UDHR is art.8. Given the widely accepted issues in the UK about access to and affordability of traditional court justice[895] and the risks involved, there is a strong case for saying that there is in real terms a lack of an effective remedy for the art.10 and art. 8 and art.6 rights engaged.

2. What should the legal liability of online platforms be for the content that they host?

a. Should online platforms be liable legally for the content that they host? In your view, are online platforms publishers or mere conduits?

(i) Publishers and conduits. The current position.

Four defences are available to internet intermediaries facing claims from third-party defamatory content: (1) the horizontal immunities under the E-Commerce Directive and implementing Regulations, (2) the statutory defence of secondary responsibility under §1 of the Defamation Act 1996, (3) common law innocent dissemination and (4) the Website Operators defence under §5 of the Defamation Act 2013.[896]The bottom line is that currently, anyone can be turned into a publisher by *actual* notice, even mere

[894] See *Equustek v Google* 2017 SCC 34 and see the EU's Article 29 Working Party issued guidance in November 2014 stating that when the RTBF is granted, results ought to be de-listed worldwide (so from .com domains too) in order to comply with the CJEU ruling in *Google Inc. v CNIL* Case C-136/17 (links to defamatory material should be removed from Google's worldwide sites on the penalty of the payment of fines by its French subsidiary). We understand that Google has so far resisted this move to implement the "right to be forgotten" on a global scale. See also *Google France Sàrl v Louis Vuitton Malletier SA* (C-236/08 to C-238/08) and *L'Oreal v eBay,* C-324/09.

[895] This is particularly so in the case of libel –where cases must be bought in the Queens Bench of the High Court and so under the full costs regime and requiring highly specialised lawyers.

[896] At present, ISPs find it challenging to rely on many primary defences as they may lack the co-operation of the authors, direct knowledge and evidence of the truth or otherwise of the allegations. Further, defences are fact intensive and expensive to prove. This renders the intermediary defences all the more attractive.

conduits, and that notice will provide such conduits with *actual* knowledge at which point they lose the immunity and other defences above, see *Twentieth Century Fox Film Corp v British Telecommunications plc* [2011] EWHC 1981 (Ch) (28 July 2011), *L'Oreal v eBay* [2009] EWHC 1094 (Ch) and *EMI Records* [2013] EWHC 379 (Ch)(blocking KAT, H33T, Fenopy)] and see also *Cartier International AG v British Sky Broadcasting Ltd* [2014] EWHC 3354 (Ch)(re trade mark infringement affirmed).[897] We set out briefly below, the position prior to such notice—by reference to trade mark cases (IP) and libel.

In any case, it depends on what the platform has done as to their legal status. If they cross a line they may lose their neutrality and become liable. With libel –that line can be continuing to publish once on notice of libelous content. With trade mark infringement cases, Google and others have been held to act as hosts when providing keyword services—on the basis that the search triggers the hosted ad. See *Google France Sàrl v Louis Vuitton Malletier* SA (above) and *L'Oreal v eBay* (above). However, in both cases the court stressed that to benefit from the Ecommerce Directive immunity, the host had to be neutral, that is, its role must be merely technical, automatic and passive and without knowledge or control. Assistance in drafting commercial messages or selecting keywords might well step over the line and provide knowledge and so jeopardize the immunity, and it was a question of fact for national courts in each case. In *L'Oreal*, the court was also asked what impact on eBay's covered hosting activities, other "unprotected" activities had, but merely reiterated that if the ISP takes an active role of such a kind as to give it knowledge of, or control over, those data then the immunity will be lost.[898] To date UK courts have compartmentalized hosting activities from other activities to give effect to the E-Commerce immunities. Other activity will not therefore necessarily jeopardize the neutrality and the immunity. See *Kaschke* [2011] 1 WLR 452 (denying summary judgment), where editorial and user generated content were combined. See also *Mulvaney v Betfair* [2009] IEHC 133 where the defendant provided a betting exchange website which also contained a chat room hosting user generated content. See also *Imran Karim v Newsquest Media Group Ltd* [2009] EWHC 3205 (editorial and user generated content), cited in *Kaschke* and *McGrath* (above), (Amazon sold books but also hosted reviews).[899]

While moderating is not fatal to the Website Operators defence, it will defeat the other defences and has been applied to the other defences in a variety of cases,[900] any

[897] The intellectual property cases have the underpinning of art. 8(3) of the Information Society Directive 2001/29/EC and the implementing §97A of the Copyright Designs and Patents Act 1988, and art. 11 of the Enforcement Directive 2004/48/EC.

[898] The failure to address the question more directly is notable as the Advocate General characterized Google as having wrongly anchored the immunities to neutrality—and disagreed that this was the correct test and contrary to the Directive's focus on the activity—not the nature of the entity, noting that in practical terms, current business models often spanned a number of the relevant activities in an industry in the process of constant change.

[899] Following *Kaschke*, if a service consists of the storage of the particular information complained of (that is, the particular post or entry complained of), the service provider is not precluded from invoking the hosting immunity merely because he also provides some other—unprotected—services, provided that the nexus between the activities does not require them to be considered together. There is little or no guidance on the boundaries rendering the nexus too proximate.

[900] In *Kaschke* (above), a host and the operator of the site corrected and amended language in user posts, and the court rightly characterized this as the exercise of editorial control. What saved the defendant in that case was the failure to edit the particular post in issue. The fact that the defendant took posts down of his own volition, scored them and rated them was not the subject of in-depth separate analysis in *Kaschke*; however, this conduct is classic moderating and a form of editorial control. In *McGrath*, Amazon narrowly escaped liability as a primary publisher as it had a moderation policy of limited pre-publication control by an automatic

manual review (by human eyes) will lose an ISP the defences --the notorious "Catch-22." Classic moderating is a form of editorial control and will render an ISP a publisher. There is no sensible way around this except as taken in the Website Operators defence. Further publishers and publication have long settled meanings in libel law and we cannot see that it would be worth tinkering with these.

Although different positions have been taken within the EU, the English courts treat search engines as conduits rather than hosts, see *Metropolitan Schools v DesignTechnica* [2009] EWHC 1765 (QB) (before notice as a search engine, Google's wholly automatic functions performed by its algorithm could not render it a publisher and it had no need of any defence). Owing to the futility of suing search engines, primary publishers often find themselves facing additional claims for the foreseeable republication by the search engines, see *Budu v BBC* [2010] EWHC 616 (QB). See *Slipper v BBC* [1991] 1 QB 283 (liability of original publisher for foreseeable republications). See also the decision of the appellate court in *Tamiz* [2013] EWCA 68 (distinguishing Google's passive role as a search engine from its role as a host. The court noted that after a takedown notice, Google as a host could be a secondary publisher). However, while this may be the case prior to notice, *after notice* even search engines must be liable based on the Blocking Order cases.

This is not as absolute as it may seem. Where there is control and financial benefit, art. 10 jurisprudence will uphold liability even *prior to notice* for hosts per *Delfi v Estonia*(No.64569/09 ECHR 2015) and *MTE and Index .hu v Hungary* No. 22947/13 (the provision of notice and takedown procedures can itself satisfy the balancing and proportionality required for the fundamental rights analysis). Note that in *Delfi,* there was effectively a finding of constructive knowledge as the hits on the site went crazy and the ad revenue with it.

Where there is a notice both ways so that the intermediary cannot tell who is right and whether there is any unlawfulness, it does not have to take any action. See *Davison v Habeeb* [2011] EWHC 3031 Parks QC (blogger.com was like a giant notice board and Google could not be familiar with postings until notified, rejected the Law Commission's gloss that unlawful meant "prima facie unlawful" and found that while Google had received a takedown notice alleging defamation, where it faced conflicting claims it was in no position to adjudicate it could not know whether there was a defence to defamation or not. Unless it knew there was a libel, it was not on notice of unlawful activity according to the Directive).[901]

(ii) Should there be liability?

filter for forbidden words or blacklisted users which if found would escalate the post for manual, human review. None of the postings complained of failed either of these tests, so they were displayed without any human intervention. As Amazon took no steps in relation to the content and no part in any decision to publish, except by way of the automatic process referred to above, it was bound to succeed under the Directive—and the claim against it was struck out. The judge noted that if there had been a manual review (human eyes) the position might have been very different, and noted the notorious "Catch-22."

[901] This was followed at first instance in *Tamiz* [2012] EWHC 449 on the e-commerce defence (Eady J. found that a bare notification that statements were defamatory would not make it apparent that they were unlawful, where no details of falsity were provided or substantiation of bare assertions, and it had no ability to consider the availability of defences to defamation, citing *L'Oreal v eBay* for the finding that art.14. of the Directive was not to be rendered redundant in every situation where notice or facts reveal an issue, given they may turn out to be unsubstantiated and imprecise). The issue was not subject to the appeal. See also *McGrath v Dawkins* [2012] EWHC 83 (a hosting case where the claimant failed to address the merits of any defences and make it apparent that the statements were unlawful under the Directive, Amazon was not on notice of libels where its processes were automated, where takedown notices were defective as to the defences and otherwise).

Notice and Takedown works very well indeed in most cases –subject to those out of the jurisdiction as noted above. It is a decent self -help remedy. Another particularly British model is the Website Operators defence in §5 of the Defamation Act 2013. This evolved from the practice of certain operators when dealing with anonymous posts. It is a facilitation model, the operator gains the defence if he forwards the complaint to the poster/author (who has to decide whether to default, consent (to takedown) or disclose (his identity to the complainant or just to the operator pending a court order for identity disclosure—and with it some court scrutiny on serious harm and real and substantial tort). The final version passed was not as good as the original proposal which was broadly as follows.

(a) For attributed statements

(i) ISPs should be obliged to publish complaints (beside the statement complained of)[902] and leave both up in order to benefit from the intermediary immunities/safe harbours and defences.

(ii) A complainant seeking removal had to apply to a court for a Takedown order –by means of *an expedited and inexpensive paper based procedure* (emphasis added)*.*

(b) For unattributed statements

(i) Statements to be takedown on receipt of complaint unless the poster/author identifies himself, in which case the statement is treated as in (a) (i) above.

(ii) The ISP could of its own volition apply for a Leave-Up or Stay-Up order on public interest grounds.

See the earlier versions of the draft regulations and the *travaux preparatoires.*[903] Art. 10 is better served in the draft model than the final. On the other hand, we know from the US copyright model, the Digital Millennia Copyright Act (DMCA) that no-one ever avails themselves of PUT BACK (which has to be done under pain of perjury) and the material is just posted elsewhere if there are strong feelings. Arguably we have a similar rule –one is always free to re-phrase and re-post and that works too and serves freedom of expression. In practice, there is nothing a complainant can do to force a Website Operator to use the defence. So it is entirely at his discretion and many are not using it. This follows the general rule –it is a defendant's decision which defence to elect.

While we note that the UN, OSCE, OAS, and ACHPR in a Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda, as well as the Manila Principles on Intermediary Liability emphasise that 'Intermediaries should never be liable for any third party content.' With respect, we think that the current position whereby the intermediary has a choice to continue to participate in the acts

[902] Known in libel law as Louchansky notices, see *Loutchansky* [2002] EWHC 2490

[903] See http://www.parliament.uk/business/committees/committees-a-z/joint select/draft-defamation-bill/news/publication-report/

complained of after being put on notice is a pragmatic and sensible one that works well for parties who are professionally represented and dealing with platforms and intermediaries within the jurisdiction.

On fake news and offence etc, it is also important to remember that art. 10 protects the right to offend, see *Handyside v the United Kingdom* App No 5493/72.[904] The ECHR has affirmed that art.10 of the Convention also protects/does not prohibit discussion or dissemination of information even if it is strongly suspected that this information might not be truthful, see *Salov v Ukraine* App no 65518/01 (ECtHR, judgement of 06 September 2005), para 113. We must be careful not to create an environment where only approved or widely held views can be online. UN Guiding Principles on Business and Human Rights state that enterprises 'should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved.'[905]Note that *Magyar Tartalomszolgáltatók Egyesülete and Index.Hu Zrt v Hungary* (above) sets out the extent to which intermediary service providers can be liable for content related to their services. The ECHR found that a 'notice-and-take-down-system could function in many cases as an appropriate tool for balancing the rights and interests of all those involved. We agree –subject to our comments above about effective remedy thereafter, but more thought needs to be given to speech related removal requests and the safeguards for art. 10 and chilling concerns.

3. How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

a. *What processes do online platforms use to moderate content that they host? Are these processes fair, accountable and transparent?*

There are still issues with moderating and ecommerce defences. Moderating does not prejudice the Website operators defence under §5 of the 2013 Defamation Act (although it is a qualified privilege and subject to malice) but the other defences would all be lost. Moderating is uncomfortable unless it is complete removal. It is editing and the paradigm activity of a publisher as noted above. Particularly with some of the US platforms, all that they will do is request you follow their moderation procedures and then decline the request for takedown. Your choices then are to turn to Google here or get a Norwich (disclosure) order here with leave to serve out of the jurisdiction (but which may be ignored in the US), you can seek the assistance of the US court, but may run into the state and federal libel shields as well as first amendment issues. See 1. above. The moderation processes are not remotely transparent. It seems in many cases that US law is applied even to content published in the UK by and about UK residents and targeting the UK and earning revenue in the UK. There is no appeal or review function and even legal letters are ignored. See 1 above.

[904] (ECHR, judgement of 7 December 1976), para 49. (the right to freedom of expression protects 'not only "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population').

[905] UN Guiding Principles on Business and Human Rights, principle 11.

b. What processes are employed by law enforcement agencies and other bodies such as the Internet Watch Foundation in overseeing the regulation of online content? Are these processes fair, accountable and transparent?

No – these processes are most certainly not fair, accountable and transparent in the UK and there has long been a serious art.10 ECHR problem. These parties (IWF and Nominet and Law Enforcement Authorities) arbitrarily restrict speech and act without any regard for basic due process.

They also fail to comply with the rules for interference with the right to freedom of expression based on the three-part test, which provides that a limitation on freedom of expression must: (a) Be provided for by law (legality); (b) Meet a legitimate aim (legitimacy); and (c) Be necessary (necessity). Limitations should always be exceptional and only be implemented if they are compliant with all the criteria. The Human Rights Committee guidance is that "the relation between right and restriction… must not be reversed."[906] It has explained that 'when a State party imposes restrictions on the exercise of freedom of expression, these may not put in jeopardy the right itself.' The starting point is that the individual is entitled to the full exercise of the right. It is then up to the state to establish – based on the criteria described above – the permissibility of a limitation on such exercise. The legitimate aims pursued should also be interpreted *stricto sensu*. The 10(2) enumerated legitimate aims are: respect of rights or reputations of others, and protection of national security, public order, public health or morals. The rights and reputations of others', generally refers to 'human rights as recognised generally in international human rights law.' Neccessity implies the existence of a 'pressing social need, see the *Sunday Times* (above) and as proportionality, the Human Rights Committee has opined that '(r)estrictions must not be overbroad.'[907] Finally, the Human Rights Committee in *Fedotova v The Russian Federation* adopted the view that a limitation ground cannot be invoked for a discriminatory purpose or applied in a discriminatory manner[908] and this prohibits discrimination on the grounds of inter alia political or other opinion.[909] The ECHR often closely considers the context of the expression in issue, but the decisive factor can also be the nature of the penalties. The ECHR confirmed in *Handyside* (above) in relation to limitations to the right to freedom of expression, it 'leaves to the Contracting States a margin of appreciation' due to their 'direct and continuous contact with the vital forces of their countries.' Nevertheless, this margin is not unlimited. The ECHR 'is empowered to give the final ruling on whether a "restriction" or "penalty" is reconcilable with freedom of expression as protected by art. 10. The domestic margin of appreciation thus goes hand in hand with a European supervision.'[910] However, the extent of the

[906] Human Rights Committee 'General Comment No. 34, Article 19: Freedoms of Opinion and Expression' (12 September 2011) CCPR/C/GC/34, para 21.

[907] Human Rights Committee General Comment No 34, para 34.

[908] *Fedotova v the Russian Federation Comm* No 1932/2010 (Human Rights Committee, views of 31 October 2012) CCPR/C/106/D/1932/2010.

[909] This position is also articulated in the Committee's General Comment No. 34, which states that laws restricting the freedom of expression must not violate the non-discrimination provisions of the Covenant. Article 26 of the ICCPR.

[910] In the European context, there is usually an *inverse* relationship between the extent of the consensus among states on the substance and scope of a limitation ground and the extent of the margin of appreciation afforded to states; the greater the consensus among states, the narrower the margin of appreciation afforded to them, see See Magnus Killander, 'Interpreting Regional Human Rights Treaties' (2010) 7 (13) SUR International Journal of Human Rights 145, 151. Additionally, when applying the margin of appreciation doctrine, courts may consider the seriousness of the right infringed, whether there is a moral controversy at stake and whether broad and deep consideration has been given to the matter by national courts, see Dominic Mcgoldrick, 'A

restriction and form of expression and will bring more scrutiny to prior restraints which require safeguards and the court will also consider whether there was an alternative means of expression. More restrictive measures are permitted for broadcast due to the power of that media, and it has found that the internet can have a greater risk for art.8 privacy and data rights than the print press and so different measures may be appropriate. The court has found there is no clear consensus in Europe on the form of permissible restrictions on the internet due to the rapidly changing environment, see *Yildirim v Turkey* App. 3111/10 (a restriction less than a ban was a violation given the importance of the internet as a tool for political expression).

More precisely, the actions of IWF and Nominet still lack a proper legal basis. That is, there is a failure of legality. Art.6 also protects from retrospective legislation and the law must be prescribed and knowable (in advance) so that citizens can regulate their conduct accordingly. An interference may count as 'prescribed by law' whether its source lies in statute or the common law but the law must be accessible and foreseeable. According to the ECHR in *The Sunday Times v the United Kingdom* App no 6538/74 (ECtHR, judgement of 26 April 1979).[911]More importantly, there is a lack of due process when the police are involved and so art.6 ECHR issues also arise. This is despite the fact that businesses can be shuttered and goodwill entirely destroyed in what may be a "taking" by the state. A notice and a hearing (before or after) must be provided at least. This is not happening largely as they police often treat the site/business as evidence or instruments of crime and seize them arbitrarily and without any process.

The public record shows and it is beyond question that Nominet is a public authority for the purposes of the Human Rights Act 1998 (HRA) and this status is reflected in the Digital Economy Act 2010 and it must act in compliance with the ECHR and the TFEU. Nominet holds .uk in trust for the nation as the delegee for the UK government. Nominet is therefore obliged to act for the public benefit and in the public interest.[912]

The legally acquired goodwill and reputation associated with the domain name cannot therefore just become illegally acquired retrospectively –just at the whim or discretion of Nominet or even law enforcement. We have the rule of law to protect us from this type of arbitrary conduct.

Both generally and given the lack of any judicial finding of any criminal or civil wrong and the lack of any due process or hearing and given the over-broad application to lawful goodwill and businesses and reputations, and also the chilling impact on Freedom of Expression -the domain name seizure and suspension is often in fact, unlawful and disproportionate. We have found in practice that the NCA/police and Nominet were not open to any review of their domain name seizures even where the issue was a technical one about the day a site ceased legal online sales and there was

Defence of the Margin of Appreciation and an Argument for Its Application by the Human Rights Committee' (2016) 65 International and Comparative Law Quarterly 21.

[911] At ⁋ 49 "Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail".

[912] This is the UK government's own view. See correspondence between BERR and Nominet Chairman at http://www.nic.uk/governance/review/. See also Digital Britain p. 193 & 194.

no actus or mens rea and no follow up arrest or charge. No process was offered and the only way to get relief would have been to sue.

Further, we have concerns about legitimacy and the balancing of the various rights required when carried out by these actors. Are the IWF, NCA and Nominet adequately applying the fundamental rights analysis and balancing the art. 8 rights of reputation and art. 10 rights to Freedom of Expression and property and business rights under arts. 16 and 17(2) of the ECHR and the Charter of Fundamental Rights (CFEU) and art.1 of the First Protocol -all of which may be engaged by these actors. The art.10 rights of customers and the public must also be considered. This balancing act is difficult even for the courts, which when it is aware from the evidence that the convention rights of persons other than the parties are engaged, then it is obliged, to take them into account. See also art. 3(2) of the Enforcement Directive and as to proportionality, *Twentieth Century Fox Film Corp v British Telecommunications plc* (No 2) [2011] EWHC 2714 (Ch), where the dangers of over-broad relief or blocking were warned against.

c. *What processes should be implemented for individuals who wish to reverse decisions to filter or block content? Who should be responsible for overseeing this?*

See above. Notice and a hearing (before or immediately after the blocking or seizure) must be provided at least.

4. What role should users play in establishing and maintaining online community standards for content and behaviour?

We don’t address this question in any detail. While they currently have an important role in flagging issues for attention, there would be serious issues with art.10 if users/the community could restrict or restrain the speech of others. There is an issue with private actors determining fundamental rights where there is no effective remedy from the same. We already noted there is a right to offend protected by art.10. See above and below.

5. What measures should online platforms adopt to ensure online safety and the protection of community values or standards, while also protecting the rights of freedom of expression and freedom of information?

This is a problematic question. Art. 10 ECHR does not just protect commonly held values but also protects and enshrines the right to offend. See above. Community values today may be so liberal as to add nothing in any event. Soft law is problematic as a restriction on speech, see above. All the more so in the hands of private actors. The existing law really should be sufficient. We have hard law restrictions on offence, revenge porn, private information, libel, harassment and intellectual property, racial and religious hatred and discrimination.

The European Commission’s Code of Conduct on Countering Illegal Hate Speech Online requires States to ‘review the majority of valid notifications for removal of illegal hate speech in less than 24 hours.’[913] We note also the positive obligations that states have

[913] European Commission 'Code of Conduct on Illegal Online Hate Speech' (31 May 2016).

to prohibit incitement to hatred under the European Union's Audiovisual Media Services Directive (AVMSD art.6) states: 'Member States shall ensure by appropriate means that audiovisual media services provided by media service providers under their jurisdiction do not contain any incitement to hatred based on race, sex, religion or nationality.'

In the UK there is the Public Order Act (Incitement to Racial Hatred), the Race Relations Act and the Racial and Religious Hatred Act –and we believe the law is currently adequate and there is no need for additional legislation. We also note that international norms suggest that for speech to qualify as hate speech, the individual concerned should intend to incite violence or unlawful action, and those actions should be imminent. See *Brandenburg v Ohio,* [cite] (and its 'imminent lawless action' test) and *Gündüz v Turkey* App No 35071/97 (ECtHR, judgement of 04 December 2003) and *Rabbae v The Netherlands* Comm No 2124/2011 (Human Rights Committee, decision of 14 July 2016) CCPR/C/117/D/2124/2011 and developments in the African[914] and Inter-American systems[915] to establish a high threshold for limitations to freedom of expression, including to prevent hate speech. We note that the UK has laws dealing with revenge porn, privacy and data, harassment, obscene publications and malicious publications. There is no need for any new legislation –in our view.

We need to consider however, the kind of environment for speech we will enjoy when enforcement is all by the private discretion of private actors. We need to think about how protections for speech offline can be fully mapped online.

Traditionally English law has been very cautious about prior restraints on speech as they may force the courts into a censor. For this reason, the rule was publish and be dammed (in damages) as it is always in theory possible to make a statement in a non-defamatory way and therefore going to the court for restraints before the language was final, was to put it in a position of censor .See *Bonnard v Perryman* (1891) 2 Ch 269 affirmed in *Green v Associated* [2004] EWCA Civ 1462 and *Mosley v UK* (ECHR considered a publisher's obligation of pre-notification of a potentially defamatory article and held that 'although punitive fines or criminal sanctions could be effective in encouraging compliance with any pre-notification requirement…these would run the risk of being incompatible with the requirements of article 10 of the Convention.' It found that such punitive fines would create a chilling effect which would be felt in the spheres of political reporting and investigative journalism, both of which attract a high level of protection under the Convention.'[916] The rule against prior restraint is not squarely applicable online –where publication is continuing, the restraint will be during and or after, restraint. However the same concerns remain –and are amplified by the fact that the restraining party will be a private actor—and one that is incentivised to remove material to obtain defences and immunities for itself.

[914] See African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression in Africa', Art XIII (2), which provides: 'Freedom of expression should not be restricted on public order or national security grounds unless there is a real risk of harm to a legitimate interest and there is a close causal link between the risk of harm and the expression.'

[915] See Inter-American Principles on Freedom of Expression, Principle 11.

[916] See also cite *Pihl v Sweden*[916] in this regard, where the ECHR found that an intermediary service provider's liability for third-party comments may have negative consequences on the comment-related environment of an Internet portal and thus a chilling effect on freedom of expression via Internet.' Similarly, *Muwema v Facebook Ireland Ltd* (High Court of Ireland, judgment of 23 August 2016) [2016] IEHC 519 (considered the liability of intermediary service providers for material published by users but decided the case based on the futility of prior restraint orders, as the information pertaining to the plaintiff was already in the public domain).

Again, safety is something else. Criminal law applies online so this should be sufficient. If this is a question about how to protect the vulnerable or children –then it should be put as such. There are others who know about children and the internet and can address this.

We note that art. 15 of the E-Commerce Directive, which states that Internet intermediaries may not be placed under a "general duty to monitor" has never been properly transposed into UK domestic law. Government has taken the position that this was not necessary, on the grounds that no UK law does place intermediaries under such a monitoring obligation. The lack of such transposition leaves UK operators exposed to the risk that law may be interpreted to allow the imposition of such a duty. This is particularly severe in relation to laws that grant courts a broad discretion to impose poorly identified duties on third parties, such as §94A of the Copyright, Design and Patents Act 1989. While the UK was a member of the EU, our ISPs had the comfort that even though art. 15 had not been transposed, UK courts were still under a duty to act in compliance with EU law. When the UK leaves the EU, this comfort is diluted (or removed, depending on transition provisions). The protection from a duty to monitor is part of the core acquis underlying Internet regulation in the UK and EU. We recommend that the government proceed to transpose it with prospective effect, as part of the preparations for leaving the EU.

6. & 7. Transparency

a. *What information should online platforms provide to users about the use of their personal data? How should it be presented?*

GDPR deals with this comprehensively.

b. *Does the GDPR, in your view, provide sufficient protection for individuals in terms of transparency in the collection and use of personal data or do we need further regulation?*

Yes --in theory. We will need to wait and see in practice. In fact, in our view, despite all the focus on social media, it is the offline players who are the worst. The banks and financial institutions are also sharing data in ways that deserve very close scrutiny.

c. *In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?*

This is a very interesting topic. It is also applicable to government and has come up under the FOIA. Most parties using algorithms, including government and police and probation and others do not fully understand yet what and how they are making use of them. There are issues about fairness and bias and a myriad of issues here. No-one has got to grips with it. The GDPR makes some attempt. It is far too early to regulate in my view.

8. Competition

a. *Is competition law effective in regulating the activities of these platforms?*

It is too soon to intervene in these new markets in our view.

b. *What risks are there for the UK post-Brexit in this regard given that most competition regulation in this field is currently carried out at the EU level?*

This will be impactful if we do not adopt reciprocal EU law and standards. We may descend into a free-for all, without adequate protections. We find in particular, that EU Intellectual Property law and the ECJ decisions, always have competition concerns at their heart. This is not a local law focus and it will be a loss. English law often overly values the rights of vested interests and incumbents and property rights and we will need to be very aware of this. It's also relevant now to considerations about regulating at such an early stage. See below, but the ECJ has struck a very sensible balance in matters such as keyword use and trade mark infringement, see *Google v Louis Vuitton* (above) and *L'Oreal v eBay* (above) (keywords are not per se infringing unless the ad fails to make identity clear, as consumers usually can understand they are being offered *an alternative* to the searched for item). Similarly, in relation to linking and embedding and copyright infringement, we got a series of very sensible decisions to the effect that if the material was up online already, to link was not infringing unless there was a new public, see *Svensson* C-466/12, *Bestwater* C-348/13 and refining the rule for business users, *GS Media* C-150/16 (not infringing even if the original linked to was uploaded without right, unless a for profit use-when the rights should be investigated). Given the importance and ubiquity of linking to the web—this was all very sensible as the man in the street could not fathom that linking could be infringing. We see very sophisticated and holistic decisions—and would probably not get these domestically.

9. International

a. What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

This will be impactful if we do not adopt reciprocal standards and protections as we have from EU law. We may descend to an environment without adequate protection for the individual. US law and institutions can be focused on corporate and business interests and individuals are often not adequately protected—this is clear from their data protection failings and we see it in ICANN also. See below. The EU has been fairly proactive when it comes to enabling and facilitating the heathy development of online markets and in our view, has struck a good balance. With the Copyright Directive, the Ecommerce Directive, other harmonisation it has looked ahead and cleared the way for a truly single market. In specialist areas such as music licensing, it has been very pro-active and pro-competition. At the same time, with issues like net neutrality, it has looked for a sensible path also. In our view, this consumer-focused law and policy is one reason for the push to leave the EU, as it often does not suit vested business interests.

b. What should be the function of international organisations in the regulation of the internet? If so, what should be the role of the United Kingdom in these international organisations?

There is a need for international co-ordination and a rule-making fora. ICANN is totally unsuitable for this purpose in our view. It has no mandate for speech, moreover, it's approach is often driven by GAC (national per country government) representatives and would see a race to the bottom for speech. Its process is slow and subject to capture by vested business interests. It is not an acceptable model due to its flawed structure which privileges intellectual property owners and in our opinion, grants double voting privileges to business interests (through the IP constituency, Business constituency and Registrars constituency). We should disclose that we have in the past participated in the IP constituency and Non-commercial users constituency and in many ICANN working groups.

11 May 2018

Bishoy Maher[917] and Rahim Talibzade[918] - written evidence (IRN0015)

What role should users and online platforms play in establishing and maintaining online community standards for combating Fake News and malicious behaviour?

1. Problem Definition:

The proliferation of fake news in everyday media outlets such as social media feeds, blogs, and online newspapers have made it challenging to identify trustworthy news sources. This global problem has exposed the vulnerability of individuals, institutions, and society to manipulations by malicious actors. "Fake news" has many definitions; however, The European Commission defines it as "intentional disinformation spread via online social platforms, broadcast news media or traditional print." It is fabricated information that mimics news media content in form but not intent.

Fake news can be classified into two main categories, these are:

1. Misinformation: Information that is false or misleading regardless of intent
2. Disinformation: Information that is purposely false, or misleading, spread with intent to deceive

Fake news takes on many forms including most prominently:

1. Factually incorrect news articles or blog posts
2. Parodies, Hoaxes, Fabricated Audio Visuals, and Memes
3. Factually inaccurate statements or reports by public figures

Studies have shown the wide array of biases present within people, which makes them susceptible to these kinds of manipulations. Research has confirmed that people prefer information that validates their pre-existing attitudes – known as selective exposure. Furthermore, people view information that coincides with their ideologies and beliefs to be more persuasive than discordant information – known as confirmation bias. Lastly, people are inclined to believe more strongly in information that pleases them – known as the desirability bias. These online platforms' business models are built around targeted-advertisements, therefore are purpose built to maximize user engagement. This often leads to social media platforms trapping their users in echo chambers, whereby the content they are served is tailored to their biases. This has in turn opened an opportunity for malicious, politically-motivated outlets to spread disinformation.

The fact that tech companies such as Facebook and Google have appropriated – and monopolised – the online advertising market has led to a pay-as-you-go business model, in which advertisers are only charged when a page is viewed or clicked on. This means that users are constantly exposed to an increasingly large collection of unregulated media content and ensures that social media companies have no incentive to play the role of "arbiters of truth." Online platforms must take responsibility, if not of the information itself, then of informing their users and making efforts to discern between types of posted content. A new system of safeguards is clearly necessary.

2. Current approaches

Current approaches include the use of state actors such as the Disinformation Review Office set up by the European Union; a network of experts, journalists, officials, NGOs, and others all collaborating to report disinformation content to EU officials. However, the review process is vague at best and further lacks clarity as to how actors are recruited to be a part of these

[917] Electrical Communications and Electronics Engineering Undergraduate student at The October University for Modern Sciences and Arts in Egypt

[918] LLB Graduate Student at The London School of Economics and Political Science

"trusted" entities. This raises public concern on whether this approach may lead to infractions on the right to freedom of speech. Furthermore, the ability of a few hundred or even thousand members of this organization to classify millions of pieces of content posted daily remains a crux to this approach.

This has led to the use of Artificial Intelligence (AI) algorithms to automate the classification of content as fake or not; however, this approach remains a double-edged sword. On the one hand, algorithms are incredibly agile and can deal with the classification of enormous amounts of data with ease. However, the algorithm must have a clear objective function - a parameter-defined task that helps it evolve. Upon solving this task, the algorithm gains experience. It then uses that experience to make slight modifications to the previous iteration's parameters in order to improve the outcome of the following iteration. This self-improving function relies heavily on the input dataset to the algorithm. That is what defines the "guidelines" upon which the algorithm acts and ultimately dictates the output classification of the algorithm. Therefore, if the "guidelines" are ambiguous the output can be **manipulated**.

This has indeed happened already; whereby malicious actors are capable of introducing their own bots to online platforms to spread targeted disinformation that takes advantage of the aforementioned biases (Cambridge Analytica) – the outcome of which is the voluntary participation of people in further spreading disinformation and ultimately the promotion of spread by the algorithm as it perceives the content as legitimate.

3. Proposal:

As seen above, the online content is difficult to regulate. This report submits that users should play a semi-formal role in maintaining certain standards and expectations of the news-labelled content. The online platforms should play an essential role in facilitating that. The suggestion of adding a small feature to classify something as News-related, an opportunity to put up the source and an ability to tag something as "Fake News" will be exemplified below.

Mechanism

An online platform implements an additional feature of content-tagging that is available once a user chooses to post something. This is aimed at users who tend to publish something that may come across as news. The feature would enable those who post to fill in a small pop-up form by ticking the boxes "News-related", "Personal", or create custom categories.

On the next line "Source", the users are asked to indicate the source where they have the information from. This could have options of pasting a hyperlink, writing "self-reported", referring to another reliable source, or mentioning a political expert who spoke of such an issue, and so on. This allows the users to make judgement of the reliability of the content even if it conforms with their biases.

When showing across newsfeed, it will clearly show something as "**News-related"** so to bring awareness that this user chose to classify their material as news. This special category would allow the separation of an opinion on a political situation and a descriptive account of the events.
To allow the online platform to retain user-friendly interface, such pop-up form will not be mandatory, and will be optional. Users who aim to come across as "News" would voluntarily fill in that form to indicate the accuracy of the source.

The other users, who are reading it, will be able to classify something as "Fake News", or add custom tags such as "Opinion" by clicking on the options next to the post. This wouldn't mean the content is deleted, as other users will be able to see that this post has a lot of Fake News tags on it and who voted for it. The online platform itself is not involved in the process of deleting or regulating such content regardless of the downvotes.

4. Existing analogy:

A popular online community Reddit has a similar score-based system[919], where people can upvote or downvote the posts. It then affects which content will be put at the top based on an amount of upvotes. In this suggestion however, the content will remain regardless of the amount of downvotes. This is to ensure that there is no self-built echo chamber[920]- a place where individuals are surrounded only by the content that people ideologically identical to them endorse.

5. What it achieves:

A small feature to classify something as News-related, an opportunity to put up the source and an ability to tag something as "Fake News" helps achieve the following.

Online Communities

The online platform is not burdened by any potential liabilities. The suggestion is entirely user-centred. The online platforms include social media, forums, and other online communities.

The community regulation and additional tagging should curb the echo chambers, that currently amplify the fake news on social media, by promoting responsible content-sharing.

This helps complement current attempts to root out the fake news by the algorithms that are currently developed for social platforms.

The interface won't be heavily affected, as ticking a box and a few more lines on sources will be a good reminder for people to be adequate when posting news-related content.

Fake bot farms' influence will be significantly reduced, as now they have to publish a source. The accountability of content sharers and creators will be subject to a user-friendly standard.

End-users

People will be more aware of the content they read, and form judgement as to how reliable a source is, where it comes from, etc. For instance, if someone writes a post and may include sources to support that, people would be able to see that this person has read sites like BBC.com, or RussiaToday. This helps raise informal, self-governing standards that are set by the community through the online platform's efforts.

This would complement the previously written[921] Anti-Fake News strategies that people could use to think about the source itself, now that they are able to check it. Upon seeing something tagged as "Fake News", users will be careful when reading such content. They are less likely to be swayed, if they see the source as lacking validity.

An absence of any particular source could suggest a person is spreading disinformation or is writing a personal opinion post. An online community is able to discern and respond by classifying it themselves. A user will now be aware that he has to come across as reliable.

8 May 2018

[919] https://www.reddit.com/wiki/faq Accessed 3 May 2018

[920] Seth Flaxman, Sharad Goel, Justin Rao, "FILTER BUBBLES, ECHO CHAMBERS, AND ONLINE NEWS CONSUMPTION" (2016) 80 Public Opinion Quarterly https://5harad.com/papers/bubbles.pdf Accessed 5th May 2018

[921] https://www.ifla.org/publications/node/11174 Accessed 6 May 2018

Dr Stephann Makri[922] – written evidence (IRN013)

Question 3 (from Tech Expert session on 26th June 2018)

(a) *In what ways does the design of internet services or interfaces affect what users see, how users make decision-making, and the decisions made about users?*

1. Carefully considered interface (and information) design is essential for ensuring online environments support user decision-making effectively; at the most extreme, 'dark patterns' in interface design are intended to trick users into signing up for services or purchasing products they did not intend to. Ambiguous information presentation or interface design that aims to 'push' users in particular directions solely for commercial benefit is undesirable from a user and ethical perspective; whether a chain of entertainment articles peppered with ads, sparked by a clickbait link from a 'legitimate' news article or a 'one-click-purchase' mechanism that encourages users to place accidental or unnecessary orders. Online content providers of all types have an ethical duty, first and foremost, to their users – to support them in making informed decisions based on their needs (rather than misleading them into making profitable ones based on the provider's needs). The need to generate income can cause tension in performing this duty, but there is arguably a middle ground that can allow content providers to provide users with information, products and services they need – without compromising on user privacy (e.g. ads produced based on tracking cookies can be unnerving to some users) and without creating an artificial, frustrating interaction dialogue between user and platform where users are forced to 'jump through hoops' to complete their tasks or access the information they need. This can ultimately lead to frustration and a reluctance to use, or return to a particular online platform. Therefore, it is in the content providers' interest to strike a useful balance between user and business needs. Putting people before profit (while not ignoring commercial needs) can encourage online platforms to prosper. There is a great responsibility for designers of information and interfaces to design in ways that promote user advocacy, while still achieving business goals.

2. 'What users see' depends on what designers allow them to see and this, in turn, depends on responsible design based on an understanding of users' information needs and based on a value system aimed at supporting their needs first and foremost, even when there are products and services for sale.

3. Decisions made about users must be grounded in trustworthy data, data that users have expressly given permission to be used to make decisions about them. Achieving the 'right' level of transparency in informing users about how their data is used to make decisions about them is a challenging problem. However, what is 'right' for one user and interface may not be right for another. A prescriptive approach to data transparency is not desirable (perhaps even not possible). Instead, designers should consider transparency as an ethical responsibility and to provide it in the most appropriate ways depending on what online platform they are

[922] Senior Lecturer in Human-Computer Interaction, City, University of London

designing and, most importantly, on the transparency needs of the users of that platform.

(b) *What is the impact of platform design on groups such as children and vulnerable adults?*

1. Principles of 'inclusive design' highlight the need to make online platforms accessible for all to avoid the marginalisation of certain user groups, including those with visual, cognitive, intellectual or mental health difficulties, the elderly and the young. While designers can potentially provide personalised (system-tailored) or customised (user-tailored) interfaces for individual users with particular inclusivity needs, this is rarely the case in most online platforms and is a shame, as this provides a means of ethical platform design that not only caters for the (often individual) needs of potentially vulnerable groups but can also act as a means of protecting these groups.

2. Designers (and online content providers) have an ethical responsibility to protect and safeguard vulnerable groups, and individuals. While content providers are not legally responsible for the content posted on their services, they cannot and should not shirt responsibility for promoting social good in the online communities they have created. An ethical approach is likely to be good for long-term business.

Question 3 (from Call Document)

How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

1. The moderation policies of online platforms have been called into question; in 2012, the BBC took the drastic decision to shut down Lonely Planet's online travel forum due to the discovery of 'uncomfortable themes' in forum posts. This highlights the importance of effective moderation. However, achieving this can be difficult as there is a need to balance community safety with freedom of speech; in the months following the reinstatement of the site, several users complained on the site that their posts, often recommending a travel guide or service, had been removed based on a more stringent moderation policy.

2. Moderation has had variable effectiveness across different types of online content platforms (from social media, to YouTube, to forums). User-based moderation (where volunteers from the user community moderate) can potentially be effective, if users are provided with clear guidelines and training on what types of content is acceptable and not-acceptable and if mechanisms are put in place to prevent moderation being abused to prevent freedom of speech. A key challenge is preventing inconsistency in moderation, to promote fairness. This is often achieved through dedicated moderators, employed by the online platforms. Clear, transparent motivation promotes fairness. Much moderation in online platforms is not as transparent as it could be; designers should consider how to express moderation decisions and rationale in the most informative and unambiguous way possible and allow users to appeal decisions on the basis of the rationale not being adequately explained, the moderation rules being incorrectly applied etc. Appeals on these bases are likely to be easier to manage than those based on subjective disagreement of the outcome (rather than incorrect application of the process).

Both representatives from the platforms and users can potentially be responsible for overseeing appeals – a peer-appeals process with a final 'appeal to platform staff' option if the original appeal is unsuccessful could be explored.

Question 4 (from Call Document)

What role should users play in establishing and maintaining online community standards for content and behaviour?

1. Users can and should play a key role in defining and monitoring online community standards for content and behaviour. The best online communities are inclusive, embracing, supportive, tolerant, kind, generous and fair – grounded in a value system that promotes community pride and success. Users have a duty to create and sustain communities that reflect and encourage these values. Online platforms should provide mechanisms to support users in creating and maintaining shared community standards. These could go beyond existing (punitive) mechanisms such as 'reporting' or 'moderating'; mentoring or coaching users who deviate from these standards to help encourage the potential adoption of shared community values could create positive change.

Question 5 (from Call Document)

What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

1. Safeguarding is arguably the most important responsibility of online community platforms, but one that most platforms are only just beginning to take seriously. It has become clear, through high-profile cases of bullying, trolling and abuse, that platforms must take sizable, active measures to promote the safety of users, particularly vulnerable groups. As this must be achieved at scale, automated approaches are necessary. But fairly 'low tech' interventions should also be made possible; a social networking contact should be able to (anonymously) express concern for another if they notice unusual or uncharacteristic behaviour. Or mechanisms could be put in place to allow parents to easily monitor the online (e.g. social media) activities of their children. Platforms could explore ways of balancing safeguarding with rights to privacy, perhaps encouraging children and parents to discuss online content and issues together.

2. Promoting freedom of expression should be balanced with promoting online safety, but safety should be the utmost priority. Requiring online platforms to (a) co-create clear, fair and transparent community guidelines with their users and (b) implement robust mechanisms for ensuring those guidelines are adhered to could help achieve this. Full censorship should be discouraged; informing posters and community members (where possible) of the broad reason(s) content was deemed inappropriate promotes transparency.
3. Transparent content creation mechanisms can potentially preserve users' legal right to Freedom of information by promoting an online culture of openness. While a tension exists with the Right to be Forgotten (as information audit trails aimed at promoting transparency should, in theory, remain as permanent as the surrounding content), a balance should be struck to allow as much transparency as possible within the necessary legal and ethical bounds.

Question 6 (from Call Document)

What information should online platforms provide to users about the use of their personal data?

1. Online platforms should move beyond existing approaches of providing only a broad indication of what personal data is being collected, used and shared and why. Providing clear, explicit information to users about what personal data is being collected and shared, how it will be used and how its collection or sharing could benefit the user and/or the online platform is important. Providing specific examples using the user's data may help users make informed decisions on consent. It is not enough to state 'we use your demographics to personalise the results you see.' Instead 'this result was promoted because other people the same age and gender regularly click on it' would be more useful. But it is especially important for online platforms to provide user-friendly mechanisms (at the interface level), so users can easily review and set their preferences (e.g. for online platforms to no longer use demographic details to promote/demote search results, not promote/demote search results based on their personal data, not make any sorts of inference based on their personal data or to delete their personal data). Providing users with as much control as they desire on their personal data, at various levels, is important. The same applies for all data held about a user, whether personal data or not.

Question 7 (from Call Document)

In what ways should online platforms be more transparent about their business practices – for example in their use of algorithms?

1. Online platforms should be accountable for the content and search results they present and decisions they make. Transparent use of algorithms is one way of achieving this. It is still, however, a major research challenge to determine how best to provide transparency to users; abstracting often complex rules in order to express them in as straightforward a manner as possible is difficult, and this should be regarded as a long-term goal of artificial intelligence research. Further complications are added by the need to keep many algorithm details confidential due to commercial sensitivity. A key principle, however, should be to encourage online platforms to be as transparent as possible – ensuring explanations are given that are presented at a suitable level of detail and clarity, without disclosing commercially sensitive information. The same principle can be applied to business practices in general; as the public trusts online platforms with their data and often permits them to use this data to make powerful decisions and inferences of considerable commercial value, online platforms owe their users more transparency and accountability surrounding how that data is used to drive business practices and decisions.

Question 4 (from Tech Expert evidence session on 26th June 2018)

(a) *What are in your opinion the likely biggest changes in the way we use and interact with internet services and internet enabled technologies in the next 5-10 years?*

(b) *What are your biggest concerns about these innovations?*

1. The continued rise of ubiquitous/pervasive computing, cloud computing, big data and artificial intelligence will see greater connectedness of internet services and internet enabled technologies. While this has enormous innovation potential, increased connectedness can put user privacy and security at risk, undermining trust. A key danger is the blurring of lines between individual internet services and enabled technologies. User data (including user-generated content) should not be allowed to flow unrestricted between services and technologies, as this would make it difficult to protect it. While existing UK law goes some way to protecting user data, internet services and enabled technologies should also have an obligation to provide users with control over their data that flows in and out, supporting the principle of opted-in informed consent (e.g. by implementing some of the transparency recommendations made earlier).

Question 5 (from Tech Expert evidence session on 26th June 2018)

(a) *What is meant by the term 'ethical by design'? What principles should be adopted to ensure 'ethical by design' standards?*

1. 'Ethical by design' is term that promotes the consideration of ethical design principles during the technology design process to ensure products and services are designed with the key ethical considerations 'baked in,' ideally 'going beyond' guidelines set by regulatory bodies (Mulvenna et al., 2017). This approach is far preferable to a box-ticking exercise where designers try to demonstrate meeting ethical design guidelines or regulations without considering ethical design from the outset.

2. The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems has proposed guidelines for the ethical design of Autonomous and Intelligent Systems (IEEE, 2018). These guidelines are underpinned by the values of *wellbeing*, *empowerment* and *freedom*. These are also important values for 'ethical by design' standards of online platforms. Principles for creating standards based on these values include:

    a. **Design to protect users' *wellbeing*** by safeguarding data through robust security measures and building in understandable, usable and useful privacy controls;

    b. **Design to *empower* users** by providing clear, transparent information on the collection, use and sharing of user data (including personal data) and on the use of algorithms for search result filtering and personalisation. Give users a central role in creating and maintaining their own online community standards on behaviour (including safety) and in monitoring those standards (e.g. through peer-based moderation);

    c. **Design to promote user *freedom*** by allowing users to control access to their data and to filtering and personalisation options that influence what information is presented to them.

IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems (2018). Ethically Aided Design: A Vision for Prioritizing Human Well-Being with Autonomous and Intelligent Systems. http://standards.ieee.org/develop/indconn/ec/ead_v2.pdf

Mulvenna, M., Boger, J., & Bond, R. (2017). Ethical by Design: A Manifesto. In *Proceedings of the European Conference on Cognitive Ergonomics 2017* (51-54). ACM.

(b) What role should be played by Government, academia and private organisations in the development of these ethical standards?

1. 'Ethical by design' standards should be co-created by Government, academia and private organisations, also with representation from users of online platforms.

Question 6 (from Tech Expert evidence session on 26th June 2018)

(a) What are the advantages and disadvantages of the use of algorithms online?

1. Algorithms have revolutionised how people find information and can support accurate decision making, which is particularly important in domains where high-accuracy is important (e.g. disease diagnosis, autonomous vehicles). However, algorithms have the potential to make (potentially fatal) errors in decision-making. They can also create 'filter bubbles' (where personalisation of search results and contents means users only get to see more information related to their stated or system-inferred interests, rather than the full information landscape) and 'echo chambers' (where beliefs are re-enforced by like-minded individuals, resulting in collective tunnel vision). These are particularly dangerous as they can create 'distortions' in information flow (e.g. through misinformation, disinformation) that can undermine the fundamental British value of democracy. It is paramount these downsides are addressed.

(b) Should algorithms be allowed to make decisions which affect humans? In particular can we design unbiased algorithms?

1. It would be extremely difficult to prevent algorithms from making decisions that affect humans, as they have been doing so (to an extent) for decades. While it may be possible with robust testing and evaluation practices to design algorithms fee from overt algorithmic bias, designers should also take care to avoid *unconscious bias*. Transparency in decision-making rationale can help to some extent. But for important decisions affecting humans (e.g. disease diagnosis), algorithmic decision-making should be supported by human checking and verification.

Question 7 (from Tech Expert evidence session on 26th June 2018)

(a) How can we effectively ensure algorithms are accountable or transparent?

1. There is much ongoing research in this area. A promising approach is through the use of 'explainable AI' (xAI) – see Hosanagar and Jair, 2018). This approach analyses the inputs used by a decision-making algorithm and reports the highest-influencing ones. However, as highlighted by Hosanagar and Jair, while providing some degree of explanation is useful, providing explanations that are very detailed is counter-productive in building user trust. The 'right' level of transparency, in terms of level of abstraction of explanation provided, is likely to vary for different types of system, user and decision.

Hosanagar, K. and Jair, V. (2018). We Need Transparency in Algorithms, But Too Much Can Backfire. Harvard Business Review. https://bit.ly/2uJTnIu

(b) Would a code of conduct for algorithmic design help?

1. It is important that creators of algorithms consider the ethical implications of their work and a code of conduct for algorithmic design would help encourage this. But most important is to engender ‘Ethical by Design’ values among all online platform designers, including algorithm designers, so that questioning the ethics of particular design decisions becomes ‘automatic’ and ingrained.

July 2018

Professor Chris Marsden – written evidence (IRN0080)

Declaration of Interests: I am a professor of internet law at the University of Sussex. I am a media board member of the Society for Computers and Law, the professional society for lawyers interested in this space, and on the stakeholder advisory committee of Nominet. Neither of those are paid roles, and I am not submitting evidence on their behalf or that of the University of Sussex. I have also advised many Governments over the years on these issues.

Q: Do we need a regulatory regime for the internet? Is it desirable? Is it possible? If it is, what form should it take, self-regulation, something more directive, such as co-regulation, or imposed direct regulation by statutory body?

My last time before a Committee of either the Lords or the other place was the joint scrutiny committee of the Communications Bill 2003. At that point we were asking when we would move away from self-regulation towards some form of co-regulation, and here we find ourselves again, 16 years after Lord Puttnam chaired that Committee.

The framework for internet law is quite old. It is based on a US law, the Communications Decency Act of 1996, so it is 22 years old, and we have dealt with the way in which it has been adapted since then. In the UK, we have the E-Commerce Regulations 2002, which are based on the Electronic Commerce Directive 2000 which itself was drafted in the last century. So the framework for internet law at least is from the last millennium, which may lead us to think that it is due for an update. We deal with several pieces of law that are much older than that. Some of the issues that arise out of the Panama Papers leak concern the breach of privacy and attorney-client privilege. Those date long before the internet.

Internet regulation broadly does not just involve the law. We are all regulated by the internet. Nudge regulation has become the issue that government talks about as a way of influencing consumers, but anyone who has been using the internet since the 1990s is aware that the internet is constantly nudging us in the direction in which various parties want us to behave[923]. It is the largest single experiment in nudge regulation that exists. Ever since the browser was invented and the first cookie was placed on a computer we have been nudged in different directions[924]. The DCMS Fake News inquiry has been talking about some pretty substantial nudging in the political sphere.

Self-regulation continues, and even in the absence of any new laws we would expect the development of the internet not to be static[925]. As I have described it to the European Commission in the past, impact assessments of internet law that ask, “What happens if we do nothing?”, do not involve stasis. The zero option is the internet

[923] Marsden, C. [2012] Internet Co-Regulation and Constitutionalism: Towards European Judicial Review International Review of Law, Computers and Technology Vol.26 No.2. pp.212-228

[924] Marsden, C. [2004] Hyperglobalized Individuals: the Internet, globalization, freedom and terrorism 6 Foresight 3 at 128-140

[925] Marsden, C. [2017] ‘How Law and Computer Science Can Work Together to Improve the Information Society: Seeking to remedy bad legislation with good science’, Communications of the ACM, Viewpoint: Law and Technology doi:10.1145/3163907

continuing to develop[926]. Our relationship with the internet, as society and as individuals, continues to develop, so the do-nothing option is not one in which nothing happens. A great deal happens, but without legislative impulse.

Co-regulation is now even used by the United States Congress to describe certain aspects of internet regulation. It is quite a broadly used term that is used not just in Brussels and Paris but here and in North America to a great extent. It actually came from Australia[927]. We have often talked about de jure co-regulation, where we have a piece of legislation in place that tells the industry, "regulate or else". A very good example is the Digital Economy Act 2010, which included two specific elements of co-regulation. One told Nominet that it will have to behave as a disinterested party. The other was to do with the Authority for Television on Demand, which was later subsumed within Ofcom but was very much a co-regulatory initiative.

De facto co-regulation exists where the regulators have used their powers of extreme persuasion. It is an area where the industry players are very aware that the regulator has power. If a telecoms company is talking to Ofcom, which regulates it formally in one area, and Ofcom wishes it to take action in another area, such as the voluntary code of conduct that was introduced on net neutrality and broadband speeds, the degree of voluntariness in that, from the point of view of the telcos, was pretty limited over the years in which it was being introduced. There can be lots of de facto co-regulation taking place as well as *de jure* co-regulation that is included in the Digital Economy Act.

Dr Nash and I wrote about content on mobile phones and co-regulation 15 years ago, so we have been talking about this for a very long period[928]. It is emerging even in areas where we may not see a legislative impulse. There is lots of interesting room to see that happening.

Ten years ago now, I constructed a Beaufort scale of co-regulation for the European Commission[929]. You will be familiar with the Beaufort scale of wind speed. The wind in this case was the degree to which the Government were breathing on the forms of self-regulation that were taking place. Zero was a calm, which would be an entirely technical standards body whose standards were formed entirely within the technical community, such as the Internet Engineering Task Force, up to a 12, which could be the forms of co-regulation that were formalised in the Digital Economy Act 2010.

Between zero and 12 there is a lot of room for us to see different elements of influence that have been exerted. Given some of the recent discussions in Select Committees, Congress and elsewhere, we are probably seeing that wind blowing a lot more strongly from Government and from Parliaments towards trying to achieve something much closer to co-regulation than to self-regulation.

[926] Marsden C., J. Cave and S. Simmons [2008] Options for and Effectiveness of Internet Self- and Co-Regulation, TR-566-EC RAND Corporation: Santa Monica, CA

[927] Marsden, C. [2011] Internet Co-regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace Cambridge University Press

[928] Marsden, C., C. Ahlert, and V. Nash [2005] Protecting Minors from Exposure to Harmful Content on Mobile Phones, for European Internet Co-regulation Network, at http://network.foruminternet.org/article.php3?id_article=24

[929] Marsden, C. with J. Cave and S. Simmons [2008] *Options for and Effectiveness of Internet Self- and Co-regulation: Phase 3 (Final) Report*, RAND-TR-566-EC, Santa Monica, CA. Prepared for the European Commission Directorate-General, Information Society and Media (DGINFSO)

As lawyers we will say something about terminology first—and then something about what we can do in practical terms. On the terminology, unfortunately the term that the media always use is ISP, which is meaningless in European law. We have ISSPs—information society service providers—as Lorna suggested. We also have telcos, an even uglier term, which are the electronic communications service providers (ECSPs)[930]. They are of a different category from the service providers themselves, and we are aware that the electronic communications service providers have always been required to have much more regulation than the standard other platforms. ECSPs are critical infrastructure and there are resilience requirements affects the way we expect them to be monitored. It is now 15 years since British Telecom first introduced the Cleanfeed system, which was an attempt to block some websites online. It was the beginning of our attempt to regulate content in this way through co-regulation, and there was much debate about that.

There was a large conference at Georgetown Law School at which 25 experts presented papers on how to regulate platforms, published in an electronic law journal[931]. The United States of America is boxed in by their Communications Decency Act 1996, even though they have attempted to amend it in a very small way. The Act talks about "online service providers" or "interactive service providers", because it was almost pre-internet.

We have three alternatives:

1. not to regulate, but the world develops without regulation.

2. to regulate all the platforms that we might be concerned about.

3. to regulate only the dominant platforms.

Where you have a relatively stable duopoly or oligopoly of companies, they lend themselves very effectively to co-regulation because you have very few industry players to influence. Market entrants are much harder to regulate. The danger is that regulation can perpetuate a duopoly or oligopoly situation.

> In February, Facebook and Google announced that between them they were going to appoint 50,000 more content moderators[932]. That sounds like a lot, but given the amount of content they deal with, it is not. It somewhat gives the lie to the idea that Artificial Intelligence and algorithms are the way we regulate content in future[933]. It is actually Mechanical Turks, people being employed—subcontracted, typically—to carry out these activities[934], and, by the way, in

[930] Marsden, C. [2018] Chapter 15 'Regulating Intermediary Liability and Network Neutrality' in I. Walden ed. *Telecommunications Law and Regulation*, Oxford, 5th edition

[931] Marsden, C. [2018] '*Prosumer Law and Network Platform Regulation: The Long View Towards Creating Offdata*', Georgetown Tech. L.R. forthcoming at http://www.georgetowntech.org/georgetown-tech-review

[932] https://www.fastcompany.com/40563782/how-a-i-anxiety-is-creating-more-jobs-for-humans

[933] Discussed by Marietje Schaake MEP in April: https://www.theguardian.com/commentisfree/2018/apr/04/algorithms-powerful-europe-response-social-media

[934] Hara, Kotaro; Adams, Abi; Milland, Kristy; Savage, Saiph; Callison-Burch, Chris; Bigham, Jeffrey [2017] A Data-Driven Analysis of Workers' Earnings on Amazon Mechanical Turk eprint arXiv:1712.05796 Conditionally accepted for inclusion in the 2018 ACM Conference on Human Factors in Computing Systems (CHI'18) Papers program

> different parts of the world where their own cultural understanding of the content they are dealing with may not be ideal[935].

We need to address this question: if we want to regulate, do we want to introduce rules that apply only to the large platforms or to all platforms? We should be aware of the danger that if you apply them to all platforms, you introduce entry barriers. If you apply them only to large platforms, you have the problems of what we might think of as some very unpleasant niche players.

Q: What part should users play in establishing and maintaining online community standards for content and behaviour?

Reporting abuse has become a difficult tool, because so many of the people whose speech we would like to restrict are simply mass-reporting people trying to stop them. Alt-right and other groups will simply report en masse somebody trying to reform their speech. The existing tools that are being used are not working very effectively.

Technology companies tell us a lot about solutions that should have been adopted but were not. Twitter had a fork in the road six years ago. It could have become a much more observant community-friendly platform then but chose not to on commercial grounds[936]. Venture capitalists used to fund these companies from their inception until they became unicorn companies that were floated on the stock market. Now they fund them from their inception until they arrive just below the merger thresholds and get bought by Facebook or Google[937]. It would interesting to know from those venture capitalists the extent to which they think they have some social responsibility to ensure that those innovations are not as user-unfriendly as they have been up to now[938].

Secondly, in order to persuade these companies to adopt technologies that prevent illegal content, you need to regulate the code on how these companies program their platforms. That is considered to be a step across the Rubicon but they do it to each other all the time. Facebook regulates the environment in which it exists and the way it controls third parties, not through unilateral contracts that it thinks it controls us with but because it controls the advertising platform. The companies are constantly regulating each other's code, and it would be useful to think about the degree to which legislators can nudge them towards a more socially responsible use of that code.

Q: How can we get the user to understand the role they are playing and to take the responsibility they should be taking and see the consequence of their actions?

There was a very interesting speech given last month by Commissioner Vestager, the European Commissioner for Competition, saying that what we have seen created in

[935] Youtube Transparency Report (2018) https://transparencyreport.google.com/youtube-policy/overview

[936] https://www.fastcompany.com/40547818/did-we-create-this-monster-how-twitter-turned-toxic

[937] Facebook is expected to take 18% of global digital ad revenue this year, compared with #Google's 31%, according to research firm @eMarketer. Monthly active users in Q1 rose to 2.2 billion, up 13% from a year earlier: https://m.investing.com/news/technology-news/facebook-quarterly-profit-beats-estimates-1414535

[938] See for venture capital response to earlier Internet regulation, 19. Marsden, C. with J. Cave, E. Nason [2006] *Assessing Indirect Impacts of the EC Proposals for Video Regulation*, RAND-TR-414-Ofcom, Santa Monica, CA. at http://www.ofcom.org.uk/research/tv/reports/videoregulation/

front of us are essentially addiction platforms[939]. All those little alerts that we get on our smartphone are little dopamine hits: we get a little reward from the fact that we think we are not alone in the world and we are being constantly alerted to new things happening. She pointed out that we allow 13 year-olds to use these platforms perfectly legally in the UK—it differs in different European countries—in a way that we have decided not to do to for alcohol, tobacco or other types of addiction. Those are her words rather than mine. The world is built on addictive substances, from tea and sugar to everything else, but we should be aware that we are doing this[940].

United States Child Online Privacy Protection Act 1998, established the age of 13. There are differing ages of consent for using platforms in different countries across Europe - Germany, for instance, insists on 16[941]. In DCMS Select Committee, Dr Aleksandr Kogan discussed how these platforms are used[942]. We should be aware of the way these platforms operate and ask some of those more profound questions about that.

A decade ago we were talking about MySpace, and today we talk about Facebook, Instagram and WhatsApp—both of them owned by Facebook. But it was not just MySpace that was supplanted by Facebook, it was also Bebo, a much more child-friendly, community-aware social network that was trying to keep to European standards. It was a US start-up by an English couple, but it tried to keep to more European standards of co-regulation and it was swept away in the Facebook tide[943]. So we have had options before.

There are alternative ways, alternative communities, that are much more privacy and community-friendly. These companies have lost. I may take a perspective which competition economists would not agree with, but my view is that these companies have won in their space. It is no longer only 10% of the population using a social network, the vast majority do, and they are all using the same one. That is not accidental; it is a feature of the technologies, not a bug. You achieve a dominant position, and once a company has that dominant position we may think about how we want to treat that company.

Q: Design of the services: Is there a new way of thinking about this, not 20th-century thinking for 21st-century situations?

I wrote a book with Ian Brown from Oxford University, who is now at the Department of Digital, called *Regulating Code*[944]. If you want to achieve meaningful results, you have to deal with the way the companies regulate us and persuade them to regulate us differently, which means persuading them to change the way they engineer their software.

[939] See https://www.b.dk/globalt/eu-commissioner-margrethe-vestager-facebook-is-designed-to-create-addiction-like

[940] Crocq, M.-A. (2007). Historical and cultural aspects of man's relationship with addictive drugs. Dialogues in Clinical Neuroscience, 9(4), 355–361.

[941] See updated map at https://www.ugent.be/re/mpor/law-technology/en/news-events/news/updategdpr

[942] Kogan, Aleksandr (2018) Written evidence submitted to DCMS Fake News Inquiry, at https://www.parliament.uk/documents/.../Written-evidence-Aleksandr-Kogan.pdf

[943] See Marsden (2011) supra at pp93-106.

[944] Marsden With Prof Ian Brown [2013] *Regulating Code: Good Governance and Better Regulation in the Information Age*, MIT Press

One of the reasons why the United States looks to us in Europe with expectancy to see if we can solve these problems is that we have specific consumer laws that deal with the online environment. I have described the need for what I described as a "prosumer law"[945]. It is an ugly term, but we are all prosumers if we ever update Facebook, Twitter or anything else, or run a blog. We are producers as well as consumers, as well as being citizens, obviously.

The European Commission is talking a lot about moving towards a much more robust framework for the online consumer. It has actually used the overarching phrase "a fair deal for consumers" as what they want to move towards[946]. In the United States, that does not play very well, as it sounds like the second President Roosevelt. Nevertheless, asking, "Okay, what do we need for prosumers?"—admittedly, as you say, 20 years after we recognised the problems—would be a much more holistic way of considering how to solve some of these problems.

Q: What processes do online platforms use to moderate the content that they host, and are those processes fair, effective and transparent? Secondly, what processes, if any, should be implemented for individuals who wish to reverse decisions and moderate content? Who should be responsible for overseeing those processes?

The first problem is that the dominant platforms are United States-based platforms, and their moderation processes are designed with a view to the First Amendment to the United States Constitution. This creates problems, because we do not share their views on hate speech and other elements. That is a major problem. We have an international law that helps us in this space, which is the Council of Europe Cybercrime Convention 2001, but the Protocol No.1 of 2003 on hate speech to the Cybercrime Convention was never signed by the United States. It ratified the Cybercrime Convention 2001 in its original form from 2001, but not the hate-speech element.

The processes are designed in California, typically, or in Seattle, depending on the company. The issue in Europe that makes this slightly more awkward is that in the United States they have been quite careful to make sure that there are requirements to put back. This relates to your second question about what happens if your content is taken down and how you appeal. There are appeal procedures that you can go through that were very carefully designed in something grandly entitled the Digital Millennium Copyright Act 1998, which was in fact the United States 1998 copyright reform, which requires put-back.

Unfortunately, even though the E-Commerce Directive is of a slightly later date, it does not have those put-back provisions. Therefore we have often described this in the past as a "shoot first, don't ask questions" provision[947]. When content is taken down in Europe, there are no requirements to appeal and put it back up again. You are simply

[945] Marsden, C. and Brown, I. (2013) Regulating Code: Towards a Prosumer Law, Computers & Law, http://www.scl.org/site.aspx?i=ed30463

[946] Vestager, M. (2018) Competition and a fair deal for consumers online, Netherlands Authority for Consumers and Markets Fifth Anniversary Conference, The Hague, 26 April https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/competition-and-fair-deal-consumers-online_en

[947] Marsden, C. with C. Ahlert, and C. Yung [2004] *How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation*, PCMLP Working Paper at http://pcmlp.socleg.ox.ac.uk/text/liberty.pdf

told by whichever service provider it is that you have breached the terms of service—at any one time we have all breached the terms of service, because they are very long unilateral contracts that inevitably we are almost always in breach of—so you do not get a chance to put it back up again.

The closest that we have been to some process that we might recognise as approximating to a legal process is the process that has been instituted by Google under the right to be forgotten law, which is the result of a court case interpreting European law. It is actually more the right to be obscure, because Google does not remove the content from the internet; it just removes it from Google searches, although that in effect removes it for most purposes from people's view.

Under that procedure, Google has dealt with about 2 million cases[948]. They can be appealed to data protection authorities and then to courts, but they go through that procedure. That is the closest thing we have had to transparency on a large scale, although we should also add all the cases that have dealt with domain names and the way those are removed from one party and given to another. There are not a great number of examples of that actually in process. I am suggesting a sort of employment creation scheme for lawyers. This is an under-lawyered area of society, so I make no apologies for that necessarily.

Q: Do you think that the use of automated content filtering systems that use algorithmic processes to identify harmful content could provide a means for effective self-regulation by platforms?

It is an open question, so I do not want to pretend that there is a definitive answer at this stage. The answer will be different next year and the year after, and the Lords Artificial Intelligence Committee has reported on some of these issues[949]. You will get an enormous number of false positives in taking material down. That is almost inevitable. It is very difficult for AI to tell the difference between a picture of fried chicken and a Labrapoodle dog, simply because of the nature of the attempts by algorithms to match these things[950]. So we will have a huge number of false positives if we rely very heavily on algorithms to filter. It will need human intervention to analyse these false positives. So as a first step, you can use AI, but Google and Facebook are employing 50,000 more people not as a job creation scheme and because of the benevolence of the companies but because they recognise that there will have to be a mixture in order to achieve any kind of aim.

One of the problems is that they are responding to a perceived need to remove more content, rather than addressing what you said in your previous question about fair process and due process in these things. I suspect they will focus on the former to the exclusion of the latter simply because of the Mechanical Turk idea: that they are subcontracting to people on very low wages. It is certainly not UK minimum wage; it is far below that. That is obviously a great deal cheaper than employing a lawyer to work out whether there should be an appeal to actually put content back online.

[948] https://transparencyreport.google.com/eu-privacy/overview

[949] https://www.parliament.uk/business/committees/committees-a-z/lords-select/ai-committee/news-parliament-2017/ai-report-published/

[950] https://www.reddit.com/r/funny/comments/6h47qr/artificial_intelligence_cant_tell_fried_chicken/

I very much agree there should be audited self-regulation, which is a form of co-regulation, being a very important element. I fear that the incentive structure that we set up will be an incentive structure for platforms to demonstrate how much content they have removed, when actually a very important additional question is, "Show us the examples of successful appeals to put content back online", in order to demonstrate that they are not simply, as I said earlier, shooting first and not asking questions, which would be their tendency.

Q: Do we leave it to the platforms to deal with the online regime, or do we need determined regulatory intervention, or even law, to make this happen?

There were two recent judgments of the European Court of Human Rights. The first was an Estonian Grand Chamber case, Delfi AS v Estonia (2015), in which, essentially, a news website was made liable for the comments that were underneath the news article. It was fined for the comments, which led news websites across Europe to think that perhaps they would have to do something: either pre-moderate, which the BBC has always done but which commercial publishers have always said would require a great deal of investment, or alternatively remove comments altogether. That case has since been followed by MTE v. Hungary (2016), which restored some kind of balance. It came to a different conclusion on the facts. So we are still stuck with the principles from Delfi, although differently applied in MTE. Without overruling Delfi (which as a lower chamber, they could not), they stepped back[951].

We face a profound issue, which is that if we do require prior approval of comments, whether it be on Twitter, a news website or wherever else, we are requiring a great deal more investment, and websites may well choose to remove comment altogether. Let us assume that it is a bad thing to remove them altogether.

Q: What information should online platforms provide to users about the use of their personal data, and how should that be presented to them? With the GDPR coming into force on 25 May, does this provide sufficient protection for individuals in the use of their data, et cetera?

I work with a much greater specialist in this area, Dr Nicolo Zingales, who has published a book called *Regulating Platforms* as a result of United Nations work[952]. Our personal data is currently regulated from Dublin and Portarlington in Ireland; it was formerly Portarlington alone, but then it moved to Dublin and Portarlington. If you are not familiar with Portarlington, it is a fairly small town in Ireland, but it is where the Irish Data Protection Commissioner was based. It has never fined Facebook or Google a euro. Fines are not the only measure of the effectiveness of statutory regulation, but you might expect something to appear as a sign of effectiveness. As things stand, we are regulated via Ireland. The DCMS inquiry on fake news is dealing with Cambridge Analytica, which is being examined by the Information Commissioner here, but not Facebook, which is still to be the responsibility of the Irish Data Protection Commissioner. That was confirmed by the group of data protection regulators, the Article 29 Working Party.

[951] Bjarnadóttir, María Rún (2017) Case Law, Strasbourg: Einarsson v Iceland, Defamation on social media and Article 8, Inforrm Blog, 14 November, at https://inforrm.org/2017/11/14/case-law-strasbourg-einarsson-v-iceland-defamation-on-social-media-and-article-8-maria-run-bjarnadottir/

[952] Belli, Luca; Francisco, Pedro Augusto P.; Zingales, Nicolo (2017) *Platform regulations: how platforms are regulated and how they regulate us*, at bibliotecadigital.fgv.br/dspace/handle/10438/19402

I am somewhat cynical about trying to introduce greater transparency. The greater the transparency, the greater the amount of information you give to users, who do not read it in the first place. We can try to afford greater transparency, but the degree to which that helps us is limited. There is current controversy about the fact that Facebook has essentially relocated the jurisdiction for non-European and non-North American users of Facebook to California, rather than to Dublin, as I think many people assumed it would do. You are told that if you do not agree to the terms of service you can no longer use Facebook. That is a fairly profound response to a failure to accept what are effectively unilateral terms. Transparency is necessary, but it is a small first step towards greater co-regulation.

We tend far too infrequently to consider the other area of great regulatory arbitrage and changes, which is the financial services industry. One element of the Sarbanes Oxley Act 2003, which regulates public listed companies in the United States, that should probably have been thought about more by internet lawyers was the placing of personal responsibility on directors of financial services companies to keep data safe in S.404. That changed enormously the culture around the risk management of data in financial services companies.

Giving directors personal responsibility to keep data safe or to do other things with it is a useful way of focusing attention. I know that many members of the Committee are directors of companies themselves and will be aware that that does focus the attention.

Q: Should there be transparency in what algorithms can be used for whatever purposes and the extent to which they can be used other business models, where arguably their use could be deemed to be fraudulent?

I want to introduce use an ugly term: replicability—the ability to replicate the result that has been achieved by YouTube or whatever company is producing the algorithm. Algorithms change all the time, and one accepts that the algorithm at one particular time, for instance for Google search, is changed constantly, and there are good reasons for it wanting to keep that as a trade secret. But you would like to be able to look at the algorithm in use at the time and, as an audit function, run it back through the data and make sure you can produce the same result. We do this in medical trials all the time; it is a basic principle of scientific inquiry. It would help us to have more faith in what is otherwise a black box that we just have to trust.

Veale, Binns and Van Kleek have been working on going beyond transparency to replicability: to be able to run the result and produce the answer that matches the answer they have[953]. You do not just want to ask the company, "Is that fair?", because it will say, "Yes, it is fair". One wishes to do it independently. If you can produce replicability, you can have much more faith in the system. However, companies will not just volunteer that. It is expensive for them to do, and if it is expensive to show people results it is even more expensive to show them results and make sure that they do not change your liability. They will not volunteer that.

[953] Veale, Michael, Reuben Binns, Max Van Kleek (2018) The General Data Protection Regulation: An Opportunity for the CHI Community? (CHI-GDPR 2018), Workshop at ACM CHI'18, 22 April 2018, Montreal, Canada, arXiv:1803.06174

Q: Is current competition law is enough, if it were properly applied, to regulate the activities of these platforms?

There is this great schism between competition lawyers and communications lawyers. It should be said that I am probably a heretic when it comes to competition law; I do not believe that competition law solves the problems in these markets, first, for reasons to do with data protection, which is clearly outwith the ambit of competition law, but, secondly, because many of the monopolies that we have seen emerge in the communications agencies have emerged so fast that the claim that they are durable, permanent monopolies would normally fail the test of competition law[954]. Competition law will not be a solution. It is actually a wonderful way of parking the issue and saying that we do not have to deal with it. We will come back in 10 years' time and see where Facebook is, and who knows where we will be in relation to Facebook at that point. That is one issue that emerges.

The other issue is Brexit. I have not mentioned the B word so far, but a lot of people in the industry were surprised to learn that we will be leaving the Digital Single Market post Brexit. That is quite a dramatic step for the UK communications industry to take. If we do, we become a rule taker from Brussels across this set of issues. One reason why people in Georgetown and other places look at us as say, "How do you solve the problem?", is because we were always considered to be problem solvers in Brussels in Digital Single Market issues. Leaving aside the cliché of the unsinkable aircraft carrier and the fact that US companies have huge investments in the UK, the assumption was that we would temper somewhat the views in Brussels that were taken by the other major party—the German-French alliance—on some of these issues. That ability to influence Brussels substantially disappears if and when we Brexit. As a third country, it will be very interesting to see the extent to which we can influence the regulation of platforms.

Brexit opens up new opportunities. I think the Secretary of State has suggested that, for the first time in a very long time, we can rewrite the Electronic Commerce Directive, which terrified almost everyone I have spoken to about it. That really is untying a Gordian knot. It will be very interesting to see what happens. We will be in a very different environment, and while I assume that the Committee will only be able to be very prospective in its discussion about what will happen post Brexit, it means that some of our stable understandings about the intervention of competition law and other things will change very rapidly.

There is another point which is that we have an Open Internet Regulation (EC/2015/2120). That introduced, first, pan-European mobile roaming, which some of us enjoy. The second element is net neutrality rules, which are in a state of some flux at the moment[955]. I sit on the advisory panel for a report on the implementation of these rules in Brussels.

[954] Marsden, C. [2016] Book Review of Katerina Maniadaki, EU Competition Law, Regulation and the Internet. The Case of Net Neutrality. Alphen aan den Rijn: Kluwer Law International, 2014. 416 pages. ISBN: 9789041141408. 53 CML Rev. 2, 571-573

[955] Marsden, C. [2017] *Network neutrality: From Policy to Law to Regulation*, Manchester University Press

A problem that will emerge if and when we leave the European Union is that we will no longer be required to follow those rules on, for example, zero rating[956]. One aspect of that that the Committee might be interested in is that when you look at mobile phone contracts in the UK at the moment, many have zero-rating on specific applications—Spotify, for example, and even Netflix, which are very large consumers of data. Most of those do not include the BBC, as a non-commercial player. There is no incentive to allow iPlayer data to be consumed freely in that way.

It will be interesting to see whether there is a divergence in the way the net neutrality rules are implemented. Ofcom wrote the rules that we have in Europe. It was the chair of the working party of BEREC. It would be interesting to see, having written the rules, if we then go outside the rules, the extent to which we conform to the rules.

Q: It is an international set of agreements that we ultimately need. Is there a natural place where that should come from? What role could the UK take in trying to establish something at a global level?

One reason why we constructed the Beaufort scale, with these 12 degrees of co-regulation, is in order to be able to move sectoral regulation up and down the scale according to conditions in society and in the market. That may be a more flexible way. One of the advantages of co-regulation is that the Government can always blame the market for not producing the results they want. They say, "We were not regulating, so it is not our failure". It is the market's failure or the user's failure, even.

I declare an interest in that I have consulted for the Organisation for Economic Co-operation and Development (OECD) over the last two years on regulation in this area[957]. Mexico at the time was the largest non-European member of the OECD, aside from the obvious United States. In terms of size of economy, we will become the largest non-aligned member of the OECD post Brexit. The OECD does some fascinating and important work in this area—not direct regulatory work but work that helps to advise on regulation—and I suggest that some of its work has been very influential in assessing what we should do about intermediary liability, for instance. It is a really interesting venue to consider the statistical evidence.

11 May 2018

[956] Marsden, C. [2016] Comparative Case Studies in Implementing Net Neutrality: A Critical Analysis of Zero Rating, SCRIPT-Ed 13:1 at http://script-ed.org/

[957] 1. OECD [2017] OECD Telecommunication and Broadcasting Review of Mexico 2017, OECD Publishing, Paris at http://dx.doi.org/10.1787/9789264278011-en

Professor Christopher Marsden, Dr Victoria Nash and Professor Lorna Woods – oral evidence (QQ 1-11)

Tuesday 24 April 2018

Watch the meeting

Members present: Lord Gilbert of Panteg (Chairman); Lord Allen of Kensington; Baroness Benjamin; Baroness Bonham-Carter of Yarnbury; The Lord Bishop of Chelmsford; Viscount Colville of Culross; Lord Goodlad; Lord Gordon of Strathblane; Baroness Kidron; Baroness McIntosh of Hudnall.

Evidence Session No. 1	Heard in Public	Questions 1 - 11

Examination of witnesses

Dr Victoria Nash, Deputy Director, Policy and Research Fellow, Oxford Internet Institute; Professor Lorna Woods, Professor of Internet Law, University of Essex; Professor Christopher Marsden, Professor of Internet Law, University of Sussex.

Q1 **The Chairman:** I welcome our witnesses to this first session of our new inquiry into the regulation of the internet. I will ask our witnesses to introduce themselves in a moment.

The inquiry is wide-ranging. We will examine how the internet is currently regulated in the UK and in other countries, with a focus on transparency and the accountability of platforms and their responsibility for the content they host. We will be looking at the role of users in establishing community standards for content and behaviour and at the effect of Brexit on internet regulation. So it is a broad inquiry, as I say.

We have held a number of previous inquiries in this subject area, and we have seen how the internet transforms the way we communicate with each other and how we consume services, but we have also seen that it can be a platform for inappropriate and sometimes illegal behaviour.

We start by asking a general question about whether the internet needs to be better regulated, bearing in mind the important balance between regulation and freedom of expression. We will ask our witnesses to address those issues.

I thank our witnesses for being with us today. Our opening witnesses are leading and eminent legal experts. They are Dr Victoria Nash, Professor Lorna Woods and Professor Christopher Marsden. I advise them that the meeting is being broadcast online and that a transcript will be taken.

I will now ask our witnesses to introduce themselves briefly and, in their opening comments, to answer a fundamental question: do we need a regulatory regime for the internet? Is it desirable? Is it possible? If it is, what form should it take? Do you favour self-regulation, something more directive, such as co-regulation, or imposed direct regulation by statutory body? Shall we start with Dr Nash?

Dr Victoria Nash: I am deputy director of the Oxford Internet Institute, which is a multidisciplinary department of the University of Oxford. We were set up in 2001 specifically to look at the societal implications of digital technologies. That is broader than the internet, obviously; it is the internet of things and AI. My role there since the very beginning has been twofold. One is to conduct research. I am a political scientist and I have worked largely on issues of child protection, child safety and freedom of expression. The second hat I wear is to keep an eye on internet policy and regulation of debates, and to contribute to the department's work, where I can, to ensure that we are well connected.

The question you asked me to kick off with obviously exercises us on a daily basis. I should probably make it clear that, by way of conflict of interest, we have received funding from some of the social media companies that you might be thinking of today. We have received far more money from the Government, through the research council, so we have conflicts of interest on both sides.

As for whether we need a new regulatory framework for the internet and whether that is desirable or possible, my personal view—I would not say I am speaking for all my colleagues here—is that we do not need a new regulatory framework at this point. What we need is to use the frameworks that we have more effectively. For me as a researcher, a key thing I have done over the years is to look at the empirical evidence on harms that arise particularly through minors' use of things like social media and internet platforms. One difficulty is that often that evidence is quite inconclusive. I were to apply a test as to whether or not new regulation is needed, I would want to be very clear that there is a new evidence base that identifies clear instances of harm and, importantly, where we can identify measures to address that. I am not convinced that we have that.

On the other hand, we clearly already have very strong legal principles in place around certain sorts of content and behaviour that are illegal and not fully enforced, and where we see perhaps a lack of full responsibility on the part of some of the bigger players in this area, even the ones that say they are very willing to co-operate—and it is important to recognise that the big companies seem to be willing to co-operate. I would like to find a way of making more of that willingness to co-operate to ensure that higher standards of responsibility are met.

In particular, I would like to see more of what you might call "procedural accountability". We have already seen examples of procedures by companies such as Facebook and Google that try to shed some light on how they deal with issues such as illegal content or requests from Governments to take down content. I am thinking of things like transparency reporting, and possibly advisory boards. The problem is that we have no means of independently auditing those activities. That is the gap.

I suggest a move away from a lack of fully enforced existing regulation and a degree of self-regulation and I wonder whether there could be more room for co-regulatory options whereby you might ask for greater transparency, more frequent transparency reports and, importantly, independent audits of the data behind those, as we have seen with the digital charter. Those might look not just at how promptly content is taken down, for example, but whether it is accurately removed. The balance between ensuring freedom of expression while also ensuring that we comply with the law is really important.

That is broadly my approach to this subject.

Professor Lorna Woods: As a brief background, I started my career in the City of London as a solicitor at the time of the duopoly review and the 1990 Broadcasting Act. Coming from a media and telecoms background, I find the internet caught in the middle. I am now a professor of internet law at the University of Essex and a member of the human rights centre there.

I am currently engaged in a project with Will Perrin, who is in the audience, I believe, and the Carnegie Trust, on reducing harms in social media. We are looking at a regulatory framework as to how that might be achieved and trying to avoid some of the questions about making platforms liable for the content of others. I will be happy to talk about that if you want, but I will just put that on the table.

As for what we have at the moment, I suppose it depends what we mean by "the internet". There is lots of regulation at lots of different levels; I suspect Chris can probably say more about the infrastructure regulation. We have net neutrality, for example, which is one form of internet regulation. There is, as Vicky has mentioned, a whole tranche of criminal law out there of varying degrees of effectiveness. Section 127 of the Communications Act, for example, has been used in relation to Twitter harassment. There is a whole range of criminal offences.

I suppose my take is different from Vicky's in that I am concerned that in the absence of effective mechanisms for people to complain, and perhaps for the quiet people to have some space, there is an overreliance on criminal mechanisms, so we end up with a situation such as the Twitter joke trial, where we think, "If there is a real issue, is it dealt with best by the criminal justice system, or is it better instead to look at something regulatory but less intrusive?" I use the word "regulatory" here to encompass everything from self-regulation to direct, top-down regulation.

I am sceptical about self-regulation. The examples of good self-regulation that are usually given—the ASA and the BBFC—are, in a way, co-regulation; they both have a statutory framework and they neighbour industry regulation. The BBFC was about the cinema operators controlling the content providers. The ASA has a similar relationship through the professional distribution chains, so I am sceptical, especially in an age where we seem to have one story after another about problems.

Particularly with social media, there may be a case for a regulatory framework that at least sets the boundaries of the information that has to be given and tackling risks. Other forms of internet, such as online selling, might have a different regime, so you may not need to take the same approach right the way across content services. Of course, some content services are already regulated. We have the proposed audiovisual media services directive, if you want to talk about Brexit, that proposes that video sharing platforms should be subject to some sort of controls with regard to hate speech.

Professor Christopher Marsden: I am a professor of internet law at the University of Sussex. I am a media board member of the Society for Computers and Law, the professional society for lawyers interested in this space, and on the stakeholder advisory committee of Nominet. Neither of those are paid roles, and I am certainly not speaking on their behalf or that of the University of Sussex. I have also advised many Governments over the years on these things. I mentioned to Dr Nash before we came into the room that my last time before a Committee of either the Lords or the other place was the joint scrutiny committee of the Communications Bill 2003. At that point we were asking when we would move away from self-regulation towards some form of co-regulation, and here we find ourselves again, 16 years after Lord Puttnam chaired that Committee. I will eventually come on to co-regulation, which in a way is my specialism.

The framework for internet law is quite old. It is based on a US law, the Communications Decency Act of 1996, so it is 22 years old, and we have dealt with the way in which it has been adapted since then. In the UK, of course, we have the E-Commerce Regulations 2002, which are based on the Electronic Commerce Directive of 2000 which itself was drafted in the last century. So the framework for internet law at least is actually from the last millennium, which may lead us to think that it is perhaps due for an update.

Of course, we deal with several pieces of law that are much older than that. I taught a class this morning in which we discussed Magna Carta. Some of the issues that arise out of the Panama Papers leak concern the breach of privacy and attorney-client privilege. Those date long before the internet. Many of the issues we deal with have a longer history.

This point has been made already, but I want to extend it; internet regulation broadly does not just involve the law. We are all regulated by the internet. Many of us are amused by the fact that nudge regulation has very much become the issue that government talks about as a way of influencing consumers, but anyone who has been using the internet since the 1990s is aware that the internet is constantly nudging us in the direction in which various parties want us to behave. It is the largest single experiment in nudge regulation that exists. Ever since the browser was invented and the first cookie was placed on a computer we have been nudged in different directions. I know that the inquiry in the other place has been talking about some pretty substantial nudging in the political sphere.

Of course, self-regulation continues. Even in the absence of any new laws we would expect the development of the internet not to be static. As I have described it to the European Commission in the past, impact assessments of internet law that ask, "What happens if we do nothing?", do not involve stasis. The zero option is the internet continuing to develop. Our relationship with the internet, as society and as individuals, continues to develop, so the do-nothing option is not one in which nothing happens. A great deal happens, but without legislative impulse.

Let me say something about co-regulation. Co-regulation is now even used by the United States Congress to describe certain aspects of internet regulation, so it is quite a broadly used term that is used not just in Brussels and Paris but here and in North America to a great extent. It actually came from Australia.

One of the interesting things about co-regulation and the extended period of time in which we have been talking about it is that we have often talked about de jure co-regulation, where we have a piece of legislation in place that tells the industry, "regulate or else". A very good example is the Digital Economy Act 2010, which included two specific elements of co-regulation. One told Nominet that it will have to behave as a disinterested party; I can talk about the details later. The other was to do with the Authority for Television on Demand, which was later subsumed within Ofcom but was very much a co-regulatory initiative.

There is also de facto co-regulation, where the regulators have used their powers of extreme persuasion. It is an area where the industry players are very aware that the regulator has power. I am not suggesting that the regulator would improperly pull those discussions into other areas, but naturally if a telecoms company is talking to Ofcom, which regulates it formally in one area, and Ofcom wishes it to take action in another area, such as one area in which I am a specialist—the voluntary code of conduct that was introduced on net neutrality and broadband speeds—the degree of voluntariness in that, from the point of view of the telcos, was pretty limited over the years in which it was being introduced. We should be aware that there can be lots of de facto co-regulation taking place as well as the formal de jure co-regulation that is included in pieces of legislation like the Digital Economy Act.

When we ask whether we are moving towards the co-regulation that we have been talking about over a 15-year period, I should say that Dr Nash and I wrote about content on mobile phones and co-regulation 15 years ago, so we have been talking about this for a very long period. It is emerging even in areas where we may not see a legislative impulse. There is lots of interesting room to see that happening.

Finally, over 10 years ago now, I constructed a Beaufort scale of co-regulation for the European Commission. You will be familiar with the Beaufort scale of wind speed. The wind in this case was the degree to which the Government were breathing on the forms of self-regulation that were taking place. Zero was a calm, which would be an entirely technical standards body whose standards were formed entirely within the technical community, such as the Internet Engineering Task Force, up to a 12, which could be the forms of co-regulation that were formalised in the Digital Economy Act.

Between zero and 12 there is a lot of room for us to see different elements of influence that have been exerted. Given some of the recent discussions in Select Committees, Congress and elsewhere, we are probably seeing that wind blowing a lot more strongly from Government and from Parliaments towards trying to achieve something much closer to co-regulation than to self-regulation.

Q2 **Lord Gordon of Strathblane:** I should first declare an interest. Many years ago I was on the board of Johnston Press and I still have a small residual shareholding. Those of you who are familiar with the fate of the local press will realise that I do not need to emphasise the word "small".

My question is on online platforms and what legal liability they should have for the content they host. Are they straightforward publishers, are they mere conduits, or are they somewhere in-between? If the answer is somewhere in-between, should they be allowed to self-define where they are on the spectrum, or are there objective criteria that we can apply to say, "You are able to control that, so you should be responsible for Y"?

Dr Victoria Nash: I am not a lawyer, so I do not look at this question from a legal perspective but more from a normative perspective. Technically, I still see these platforms as mere conduits, but you can see that on child abuse imagery, for example, companies have stepped up to the mark and proved themselves willing to take on greater responsibility. You may have heard of a technique called photo DNA which you can use to test imagery on your sites to see if it has been previously identified as child abuse imagery. That is an example of active searching for illegal material.

I do, however, really fear the extension of this principle to social media and internet platforms as a whole for a couple of reasons. One is that, quite simply, one of the greatest benefits, as well as the greatest trials, of social media and the internet is the ability to provide user-generated content. We have never had an opportunity to have so many people having a say—to find, produce and share content and things they are interested in—and I would be very wary of setting up a new system that threatened that in any way.

To that extent, I would be reluctant to extend the principle of liability. I am prepared to accept it on issues such as child abuse, simply because that is an area where the proven harms are so great that it may be worth a bit of censorship, and the risk that some content may erroneously get prevented from being uploaded. But I would be very worried if we were to extend that to other areas.

I guess we are already talking about copyright, but if you were liable for any form of extremist speech, if you had to filter that out at source rather than having it reported to you, I would be worried that you would catch legitimate political speech, for example. I do not have enough faith in our technical measures, our means of detecting content and what is in content, and I certainly do not think you can employ enough human moderators to read everything that we host online. For that reason, I see very little value in making these companies liable for every bit of content that we, as users, post.

Lord Gordon of Strathblane: I will just ask you to respond to something that has been in the news recently. People are saying that knife crime has been prompted to some extent by what people are saying on social media. Would that not warrant some kind of intervention by somebody?

Dr Victoria Nash: I have also heard interviews on Radio 4 saying that it is down to rap music. The first thing I would want to know is that there is clear evidence that these harms are being exacerbated. Secondly, I would want to know that whatever response you take is proportional. I would worry that the response of checking every piece of content for a reference to knife crime before it goes online would have a damaging, censoring effect.

Professor Lorna Woods: On the e-commerce directive and platforms, I think there is an issue with terminology. We now talk a lot about platforms, but there is not, to my knowledge, a legal definition.

Lord Gordon of Strathblane: Quite.

Professor Lorna Woods: The e-commerce directive actually refers to "information society services", so to fall within the immunity from liability you have to be an information society service to start with. Not all things that I would consider to be a platform are information society services. Uber is the obvious example: it is a platform, not an information society service, according to the Court of Justice. There is a question there about fit.

On the issue of immunity from liability, I would like to move away from the question, "Is it purely about transmission or is it about content?", to a different analogy whereby we say that they are providing us a space, like a pub, a park or a shopping centre. In thinking about the responsibilities of a social media company in particular, perhaps the analogy of the space and what we expect people who provide spaces to do would be more helpful.

Lord Gordon of Strathblane: We expect a space to be safe: health and safety would apply.

Professor Lorna Woods: Yes, and part of what Will Perrin and I are thinking about is that maybe we should look more at the systemic level and say that the companies that provide online services should look at what they are providing and whether it is reasonably safe. Rather than spending a lot of time deriving algorithms that push extremist content up the autoplay list, they might go for something that is perhaps a little more society-neutral.

However, this moves away from a model that says they are liable for the speaker's content. It is saying that they have a responsibility for the space and should focus much more on that rather than on individual instances of identifiable bad content. There will always be a link, obviously, and if there are lots of problems you might say that that indicates that you have a poor system underneath.

If a platform is notified of problematic content—let us assume that we all agree that it is problematic content—and they do nothing, do we still say that they should be immune, or do we say that it is the sign of a bad system? There are questions here about how the interplay between the system and an individual instance of content would work out. Obviously, at the moment, for the system, they should take down promptly content of which they are aware, and there is a question about the effectiveness of the current system anyway.

That is a different problem. It goes partly to questions about transparency of processes: we do not know how they are monitoring stuff and whether they are prioritising some forms of content over others. So we will look at some speakers more swiftly, and other speakers, because they have a big audience, more slowly: "We give this speaker more leeway than that speaker". We do not know whether they are doing that.

So I agree that we should have more information, but it should be less at the grace of the social media company and more required in an organised and systematic manner, so that we can actually understand what is going on.

Professor Christopher Marsden: I want to say something on the terminology—of course, as lawyers we will say something about terminology first—and then something about what we can do in practical terms.

On the terminology, unfortunately the term that the media always use is ISP, which is meaningless in European law. We have ISSPs—information society service providers—as Lorna suggested. We also have telcos, an even uglier term, which is the electronic communications service providers (ECSPs). They are of a different category from the service providers themselves, and we are aware that the electronic communications service providers have always been required to have much more regulation than the standard other platforms.

This dates back to the days of telco regulation, and the fact that they are critical infrastructure and there are resilience requirements affects the way we expect them to be monitored. Also, of course, we remember that it is now 15 years since British Telecom first introduced the Cleanfeed system, which was an attempt to block some websites online. It was the beginning of our attempt to regulate content in this way through co-regulation, and there was much debate about that.

I am very happy to share with the Committee the fact that there was a large conference at Georgetown Law School two months ago at which 25 experts presented papers on how to regulate platforms. They are about to be published in an electronic law journal, so I will provide the Committee with that. The American speakers at the conference—they were speakers from the United States of America, I should say, rather than from other parts of the Americas—were looking to the UK for solutions. They are boxed in by their Communications Decency Act of 1996, even though they have attempted to amend it in a very small way. The Act talks about "online service providers" or "interactive service providers", because it was almost pre-internet.

We have three alternatives. One is not to regulate, but of course that means that the world develops without regulation. The second is that we can regulate all the platforms that we might be concerned about. The third is to regulate only the dominant platforms. One element that we need to be very aware of—it is not just an internet phenomenon, it is much more broad, but it plays out very strongly with the internet—is that, where you have a relatively stable duopoly or oligopoly of companies, they lend themselves very effectively to co-regulation because, of course, you have very few industry players that you have to influence. Obviously market entrants are much harder to regulate. The danger is that you want to regulate, but that when you do you are almost perpetuating a duopoly or oligopoly situation.

So, yes, we might want to regulate Facebook and Google. In February, Facebook and Google announced that between them they were going to appoint 50,000 more content moderators. That sounds like a lot, but given the amount of content they deal with, it is not. It somewhat gives the lie to the idea that artificial intelligence and algorithms are the way we regulate content in future. It is actually Mechanical Turks, people being employed—subcontracted, typically—to carry out these activities, and, by the way, in different parts of the world where their own cultural understanding of the content they are dealing with may not be ideal.

We need to address this question: if we want to regulate, do we want to introduce rules that apply only to the large platforms or to all platforms? We should be aware of the danger that if you apply them to all platforms, you introduce entry barriers. If you apply them only to large platforms, you have the problems of what we might think of as some very unpleasant niche players.

Q3 **Baroness Bonham-Carter of Yarnbury:** I want to return to Lord Gordon's initial question as to whether online platforms are publishers or mere conduits. I take Professor Woods' point that there is a lack of a legal definition of a platform. I did not really appreciate that before. What about the use or misuse of a person's name, their reputation, without their permission, to sell a product? It is what I think we call fake adverts. Should the platform not take responsibility in that case?

Professor Lorna Woods: The system we have from the electronic commerce directive distinguishes broadly between criminal wrongs and civil wrongs, so a harassment claim could be criminal where defamation is civil. Apart from that, the regime, in terms of immunity from liability, is pretty much the same. It applies to a neutral intermediary when we are talking about a host, which we are on most of these platforms.

There is the question of what "neutral" means, and whether the prioritisation of content, for example by algorithms, is neutral or not. But if we assume that we have a neutral conduit, it has immunity, in the case of criminal law until they actually know about it, or in the case of civil law until they should have known about it or they actually did know about it. Then they must take the content down—or block it or deal with it—expeditiously. But there are questions about what that means when they actually have knowledge. One of the issues is that a lot of the big platforms say, "We have so much data that we cannot actually know".

Baroness Bonham-Carter of Yarnbury: Do you believe that?

Professor Lorna Woods: They could probably do more. I am not a technologist, but my suspicion is that if I were a business person I would try the argument that I cannot know to put off the evil day of trying to work out how to fix the problem. I am perhaps a little sceptical of "cannot know". Certainly, there are techniques that are now being used in terrorism and in relation to child pornography in order to keep content down: identifying or watermarking content so that it does not pop up again.

There is a question about whether platforms should be able to just take content down once or whether, once they become aware of it, it should be taken down and stay down.

The consequence of the regime is what I think you are alluding to, which is that it puts the onus on the individual—the victim, if you like—to keep an eye out for problem content and then to persuade the platform to do something about it. That is a problem, especially if you are talking about revenge pornography or something like that. It is really hurtful to expect someone to have to monitor. In the case of the advertising you mentioned, I think there are probably financial costs for somebody whose reputation is—

Baroness Bonham-Carter of Yarnbury: It is a form of identity theft.

Professor Lorna Woods: Yes.

The Lord Bishop of Chelmsford: I wanted to come back to something Dr Nash was saying. I think Professor Marsden started to answer the question that was forming in my mind. You mentioned that child pornography is harmful. It is indeed extremely harmful, and there are other things that Lord Gordon also referred to: hate speech, knife crime, terrorism and all the rest. I think I heard you say that while it would clearly be good for this to be taken down, we do not want to run the risk of damaging people who are making legitimate things, and we cannot read everything.

The platforms cannot have it both ways. They cannot on the one hand be the people through whom we have to access everything on the internet—that is who they want to be; that is the world they have created—and then say that they cannot be responsible for the content. You say that they cannot employ thousands of people to read everything, although now I learn that that is exactly what they are doing.

Could it not be the other round? Actually, there could be a much more rigorous form of blocking and monitoring content. Then, if a mistake is made, which is bound to happen, the person whose content is blocked applies to say, "Actually, this stuff is entirely innocent. Could you please unblock me?" Why does it have to be this way round?

It felt like your answer was pretty complacent about the real dangers. This is what we could and should be doing on what is a hugely serious and damaging range of issues.

Dr Victoria Nash: I certainly did not mean to sound complacent. Let us have a thought experiment. You ask whether it could be the other way around. Certainly someone could set up a platform, a system today, that would do precisely that. That is precisely what some of the platforms that are focused specifically on children do: they provide a safe space in which content is all moderated, or you can only use certain forms of language, or individuals are white listed. A variety of platforms already do that, but they tend to do it only for children. You could do that for adults, but clearly it would have some pretty big implications.

The idea that everything I might want to say about my family, my friends, my life, would have to be read by a human moderator before it could be posted on a site—

The Lord Bishop of Chelmsford: No, that is not what I am saying. That is an extreme version of what I am saying. I am asking whether there could be a more sophisticated and rigorous way of monitoring what could be damaging and extreme content—and therefore accepting the risk that sometimes quite legitimate content slips through—but also a very clear and transparent way of appealing if my contents had been blocked and that turned out to be right. Then the human element would come in to read it. In other words, turn that whole thing on its head.

Dr Victoria Nash: Just to be clear, you are suggesting a system whereby, again, every bit of content that we want to share would be checked in advance but artificially using algorithms and AI. Is that right? Something like that.

The Lord Bishop of Chelmsford: Yes. They are doing it anyway for their own purposes, are they not? It is not as though this is a new thing to do, is it? It is just a different algorithm. It is not a whole new bit of work. It is just as bit of responsibility.

Dr Victoria Nash: All I can say is that it sounds like a really easy solution. Yet every bit of experience I have ever had with computer- science technologists showing us how you do this suggests that it is remarkably difficult to identify when content falls into a bucket that is so clearly harmful, or maybe just offensive, or maybe clearly fine.

One example is hate speech. A very good research project at the University of Cardiff is trying to identify examples of hate speech on Twitter. It was very interesting to note that while they were trying to train their algorithms to identify it, they worked with a panel of experts, and that even that panel of experts agreed only 75% or 80% of the time, and that was even before getting to training the algorithms.

I suppose my point at the moment is that the technology is not there, this would be heavily restrictive from the perspective of freedom of expressions, and, quite frankly, it would place the UK not at the forefront of safety but very much at the forefront of potential censorship, and I would worry about that.

The Chairman: Thank you. We move on to another question, from Baroness Benjamin.

Q4 **Baroness Benjamin:** We are all aware of, and you have mentioned already, how platforms such as Twitter enable abusive behaviour that you would perhaps not engage in face to face and but feel that you can online. The Government's digital charter states that people should understand the rules that apply to them when they are online, and it commits the Government to protecting people from harmful content and behaviour and is working with industry to encourage the development of technological solutions, which you mentioned.

However, do you not think that users themselves need to play a part? What part should they be playing in establishing and maintaining online community standards for content and behaviour, and should there be some sort of rule book that they need to follow or at least be aware of?

Dr Victoria Nash: Yes, I think there should be. Technically there are. Most of the services that we use have community guidelines or community standards that we are supposed to abide by as users. As I understand it, again there are examples of initiatives by companies that are trying to understand the patterns of behaviour we see here and how we might intervene, as you say, to prevent individuals harassing each other and using abusive language. I cannot remember which companies; one might be Jigsaw, which is talking for example about identifying key words. Instead of preventing you from using those words, it might give you a nudge, a prompt: "Do you really want to use that word? It doesn't seem to abide by community standards", et cetera.

The companies could do more perhaps to remind us of those community standards when we are using their services. But, frankly, I also think that we need to do more on the education and parenting side, and we need a much better understanding of exactly what drives people to be quite so vile to each other in this environment. I presume you are asking about both sides, and this is not just a regulatory question but a social question.

Professor Lorna Woods: It is a very interesting question. The dominant companies talk about community standards, but they are not community standards; they are terms of service imposed on their users.

In the case of Facebook or Twitter, it is not about what their users think. There are other platforms that give the users the freedom, within an overarching framework that is about legal content and so on, to set their own standards. Have you heard of Mastodon? It is a Twitter-alike, so it is short communications but it is based on a peering system. Somebody who has the computer space downloads the software and can run an instance of Mastodon. Each of those instances can set its own rules.

British Mastodon says, "We're all up for robust speech", which I take as code for shouting at each other. Other groups say expressly "We don't allow that". There is a vegan group that says, "You have to accept the principles of veganism". The feed is based on that user group, but individually you can also subscribe to other groups, so it is not totally fragmenting.

There are possibilities out there. The problem at the moment is that there is too much power in the hands of the big platforms, which are using the phrase "community standards" in one sense but still nudging us towards a whole range of behaviours in another. They are just using community standards as their justification for taking stuff down.

I agree with you that other tools can be invented and about looking at some of what women said about the abuse. Part of the problem is that you cannot mute before you see it, so why has nobody really come up with a system so that as a user you can choose to block categories of content that you do not want to see?

Professor Christopher Marsden: There are two things to say about that. I think we are now realising the value of disgruntled former employees of technology companies telling us a lot about solutions that should have been adopted but were not. As I understand it, Twitter had a fork in the road six years ago. It could have become a much more observant community-friendly platform then but chose not to on commercial grounds.

Venture capitalists used to fund these companies from their inception until they became unicorn companies that were floated on the stock market. Now they fund them from their inception until they arrive just below the merger thresholds and get bought by Facebook or Google. It would interesting to know from those venture capitalists the extent to which they think they have some social responsibility to ensure that those innovations are not as user-unfriendly as they have been up to now. There is a whole separate question about why people are so extraordinarily vile to each other online. That is something for psychologists to help us to discuss. I think that people have been vile to each other from an extraordinarily long period of time, but it is very interesting to see this irrefutable evidence in front of us of just how awful people are being.

Secondly, in order to persuade these companies to adopt technologies that enable you prevent this content from being seen in the first place, you need to regulate the code on how these companies program their platforms. That is considered to be some kind of step across the Rubicon and an awful thing to do. They do it to each other all the time. One thing that we have learned over the last couple of months is the extent to which Facebook regulates the environment in which it exists and the way it controls third parties, not through unilateral contracts that it thinks it controls us with but simply because it controls the advertising platform.

The companies are constantly regulating each other's code, and it would be useful to think about the degree to which we can nudge them—to use that overused expression—towards a more socially responsible use of that code. One of the people who might give you some insights into that might be Sir Tim Berners-Lee, who obviously has a 25-year history of thinking about these things and being publicly very unhappy about the way his baby is being brought up by some of the technology companies. Certainly in the case of Twitter, there was a fork in the road—a point at which it could have done something.

Unfortunately, reporting abuse has become a difficult tool, because so many of the people whose speech we would like to restrict are simply mass-reporting people trying to stop them. So we have this awful situation where alt-right and other groups will simply report en masse somebody trying to reform their speech. So the existing tools that are being used are not working very effectively.

Baroness Benjamin: When we think about the user, many people do not fully understand what they are doing. There are the extremists—they know exactly what they are doing—but for the innocent, children and young people especially, do you think that education is what is needed? Do you think we may drive them to their own dark place that they create themselves where they can be abusive? For instance, on Instagram there is a place where children can go and abuse other children: adults cannot get to it but children can.

The other thing that worries me is whether we will drive people to a system such as WhatsApp: you can do things there that nobody can see. How do you think we can get the user to understand the role they are playing and to take the responsibility they should be taking and see the consequence of their actions?

Dr Victoria Nash: Obviously, since I have been in this space, particularly over the last 10 years, we have seen a proliferation of calls for more digital literacy training. I know it is an Ofcom responsibility, but one thing we lack in this area is that there is not a great deal of evaluation of the interventions that are made or the training programmes that are introduced. This is a big gap at the moment.

You are absolutely right that we need to work far more closely with children, through schools and in out of school programmes, but we could also do a better job of evaluating what we are currently doing and seeing what works in transforming behaviour and in helping children understand the consequences of their actions.

Maybe I can put this a bit more starkly than you did. There is a real danger that someone who is really determined to attack another individual, to bully or harass them, will find a way of doing so. You may make it hard for them to do it on Facebook, but you are right: it is like a game of whack a mole—you shut down that route and they will move on to Instagram or WhatsApp or an even more private channel.

The only solution is the educational and the societal one. That does not mean that we should not act on the other angles too, but I think that is the only one by which we have a real chance of success. The key measures would be massively more funds available for digital literacy training. I know PHSE is coming back up the political agenda, which is great, but we also need more evaluation of the types of scheme we put in place to ensure they are actually working in transforming behaviour.

Professor Christopher Marsden: There was a very interesting speech given last month by Commissioner Vestager, the European Commissioner for Competition, saying that what we have seen created in front of us are essentially addiction platforms. All those little alerts that we get on our smartphone are little dopamine hits: we get a little reward from the fact that we think we are not alone in the world and we are being constantly alerted to new things happening. She pointed out that we allow 13 year-olds to use these platforms perfectly legally in the UK—it differs in different European countries—in a way that we have decided not to do to for alcohol, tobacco or other types of addiction. Those are her words rather than mine. And, of course, the world is built on addictive substances, from tea and sugar to everything else, but we should be aware that we are doing this.

We are doing it, actually, because of a United States law, the Child Online Privacy Protection Act 1998, which established the age of 13. We have chosen to do that. We have differing ages of consent for using platforms in different countries across Europe. Germany, for instance, insists on 16. And we are very aware, of course, that children under the age of 13 are signing up to these platforms, with or without their parents' knowledge. We should just be aware of that. It is interesting to note that this morning in a Select Committee of the other place a psychologist was talking about the way these platforms are used. We should be aware of the way these platforms operate and perhaps ask some of those more profound questions about that.

I just make one note: 10 years ago we were talking about MySpace, and today we talk about Facebook, Instagram and WhatsApp—both of them, of course, owned by Facebook. But at the time it was not just MySpace that was supplanted by Facebook, it was also Bebo, a much more child-friendly, community-aware social network that was trying to keep to European standards. It was a US start-up by an English couple, but it tried to keep to more European standards of co-regulation and it was swept away in the Facebook tide. So we have had option before.

Yes, there are alternative ways, alternative communities, that are much more privacy and community-friendly. These companies have won. I may take a perspective which competition economists would not agree with, but my view is that these companies have won in their space. It is no longer only 10% of the population using a social network, the vast majority do, and they are all using the same one. That is not accidental; it is a feature of the technologies, not a bug. You achieve a dominant position, and once a company has that dominant position we may think about how we want to treat that company.

Q5 **Baroness Kidron:** I am afraid that I have to declare interests before I ask my question, which is on the back of what you just said. I am the founder of 5Rights and I am working on universal data standards with many international partners. I brought various amendments to the Data Protection Act on the subject. I am a member of the broadband commission on the sustainable development goals and the Royal Foundation's task force on bullying. I am a director of Freeformers, which is a digital transformation company. I run workshops with children to capture their thinking about the digital environment and I am currently working on and about to publish something about persuasive technology. Sorry about all that.

I was going to ask all of you about the very point that you have made, which is that when we first asked whether these companies should be regulated, everybody took that to be from a content point of view. However, we are increasing the understanding that this is very addictive technology. In fact, the various addictions sit in regulatory frameworks of various kinds. I do not want to use the Bishop's word, but why did we just accept that? Why are we suddenly saying, "Oh, well, they have won"? Are we ready, and is this the moment, to look at some of the asymmetries of the situation?

I suppose my precise question is this. Do you not think that when we talk about regulation we have to talk about the design of the services as well as the content?

My second question is closely related to that. At various points in your answers you grasped at existing laws, but we are talking about a new space. When we asked whether we should have a new regulatory framework, Professor Woods said that its space is its otherness, but should we not be more imaginative and ask about proportionality and things that are monetised above a certain point? Is there not a whole new way of thinking about this, rather than grasping at 20th-century thinking for a 21st-century situation?

Professor Christopher Marsden: Yes, there is obviously a lot to unpack. I wrote a book five years ago with Ian Brown from Oxford University, who is now at the Department of Digital, called *Regulating Code*. I agree that if you want to achieve meaningful results, you have to deal with the way the companies regulate us and persuade them to regulate us differently, which means persuading them to change the way they engineer their software.

On the other point about whether we should be thinking much more seriously in relation to the framework, one of the reasons why the United States looks to us in Europe with expectancy to see if we can solve these problems is that we have specific consumer laws that deal with the online environment. I have described the need for what I described as a "prosumer law". It is an ugly term, but we are all prosumers if we ever update Facebook, Twitter or anything else, or run a blog. We are producers as well as consumers, as well as being citizens, obviously.

The European Commission is talking a lot about moving towards a much more robust framework for the online consumer. It has actually used the overarching phrase "a fair deal for consumers" as what they want to move towards. In the United States, that does not play very well, as it sounds like the second President Roosevelt. Nevertheless, asking, "Okay, what do we need for prosumers?"—admittedly, as you say, 20 years after we recognised the problems—would be a much more holistic way of considering how to solve some of these problems.

Professor Lorna Woods: I said that the spaces analogy, the project I am working on, is looking at the systemic level. That implies that as well as looking at techniques for blocking and such like, it is also looking at the actual structure of the platform and the nudges and the way they encourage us to stay engaged. It is very much in line with what Chris is talking about when he talks about code. I just wonder whether it would help the Committee if I sent through an outline of what we are trying to develop.

The Chairman: I think the Committee would find that very useful. Thank you.

Dr Victoria Nash: I am not sure that I have any other great insights to add to what has already been said.

Baroness Benjamin: I did not declare my interest before I asked my question. I am a champion of the Internet Watch Foundation and a vice-president of Barnardo's.

The Chairman: Thank you for doing that. I apologise to Lord Goodlad, who I inadvertently slipped down the order of questions. He will ask the next question.

Q6 **Lord Goodlad:** Can I ask my question in two parts, please? First, what processes do online platforms use to moderate the content that they host, and are those processes fair, effective and transparent?

Secondly, what processes, if any, should be implemented for individuals who wish to reverse decisions and moderate content? Who should be responsible for overseeing those processes?

Professor Christopher Marsden: The first problem is that the dominant platforms, of course, are United States-based platforms, and their moderation processes are designed with a view to the First Amendment to the United States Constitution. This, of course, creates problems, because we do not share their views on hate speech and other elements. That is a major problem. We have an international law that helps us in this space, which is the Council of Europe's Cybercrime Convention 2001, but the protocol on hate speech to the Cybercrime Convention was never signed by the United States. It signed the cybercrime treaty in its original form from 2001, but not the hate-speech element.

The processes are designed in California, typically, or perhaps in Seattle, depending on the company. The issue in Europe that makes this slightly more awkward is that in the United States they have been quite careful to make sure that there are requirements to put back. This relates to your second question about what happens if your content is taken down and how you appeal. There are appeal procedures that you can go through that were very carefully designed in something grandly entitled the Digital Millennium Copyright Act 1998, which was in fact the United States 1998 copyright reform, which requires put-back.

Unfortunately, even though the E-Commerce Directive is of a slightly later date, it does not have those put-back provisions. Therefore we have often described this in the past as a "shoot first, don't ask questions" provision. This may answer some of the points which the Bishop made. When content is taken down in Europe, there are no requirements to appeal and put it back up again. You are simply told by whichever service provider it is that you have breached the terms of service—by the way, I imagine that at any one time we have all breached the terms of service, because they are very long unilateral contracts that inevitably we are almost always in breach of—so you do not get a chance to put it back up again.

The closest that we have been to some process that we might recognise as approximating to a legal process is the process that has been instituted by Google under the right to be forgotten law, which is the result of a court case interpreting European law. It is actually more the right to be obscure, because of course Google does not remove the content from the internet; it just removes it from Google searches, although that in effect removes it for most purposes from people's view.

Under that procedure, Google has dealt with about 2 million cases. They can of course be appealed to data protection authorities and then to courts, but they go through that procedure. That is the closest thing we have had to transparency on a large scale, although I suppose we should also add all the cases that have dealt with domain names and the way those are removed from one party and given to another. That is another example of it happening. But there are not a great number of examples of that actually in process. I realise that I am suggesting a sort of employment creation scheme for lawyers. This is an under-lawyered area of society, so I make no apologies for that necessarily.

Professor Lorna Woods: There is an underlying issue, which is that the whole system is set up by contract, and the companies are not required to do any of that. Bizarrely, if we had thought more about the regulatory framework we could have had a better job. I reiterate what Chris has said about the complete lack of transparency about what happens, who does it and on what basis. We just do not know.

There is an assumption—this is perhaps moving slightly from the question—that platforms are there for us to speak on, so when people talk about freedom of expression it is almost as though the user has a freedom-of-expression right as against the platform. There is no such thing. As a matter of law, rights bite against the Government, not against the company, so you are in the land of positive obligations where the obligations are harder to prove than in the case of a complaint against the state.

Looking more broadly, if you are looking for some sort of regulatory framework, you could look at the essential facilities doctrines from competition law, but although they allow third-party access to private platforms of various sorts, I do not think they would cover this sort of situation. So there is a gap.

Dr Victoria Nash: I think you have beautifully explained why we have this problem. For me, this is a significant area of concern. Given everything we know about the digital charter and the concerns of this Committee, it is very likely that in the future we will ask these private sheriffs, these private companies, to act and take down more and more content in order to comply with the law as well as their community standards.

We could certainly make more progress in two ways, and here I must declare another conflict of interest in that I am involved in an initiative that is planning to do some of this work. First, we could provide guidance on what consumers and users ought to be told and how they are told when their content is taken down, and ideally put measures in place for appeal—the idea that that is part of being a responsible platform in this area.

Secondly, it might be beneficial—and this would probably require regulatory oversight—to have some sort of auditing of this process by an independent third party. I suggest two types of auditing: first, an auditing of the companies' decisions to remove content to ensure that it meets the complaint that was made or breaks the law that was suggested; and secondly, perhaps, also an auditing of moderation guidelines, again in order to have oversight of the processes and procedures behind these decisions. That would fill a significant gap and help to assuage some of the concerns about chilling effects or unintended consequences of legal and legitimate speech or acts being closed down untransparently.

Lord Goodlad: That is extremely helpful. Do you think that the use of automated content filtering systems that use algorithmic processes to identify harmful content could provide a means for effective self-regulation by platforms?

Professor Christopher Marsden: It is of course an open question, so I do not want to pretend that there is a definitive answer at this stage. The answer will be different next year and the year after, and the Artificial Intelligence Committee has reported on some of these issues.

You will get an enormous number of false positives in taking material down. That is almost inevitable. I do not know whether you have seen the Labrapoodle pages that have shown you that it is very difficult to tell the difference between a picture of an Orangutan and a Labrapoodle, simply because of the nature of the attempts by algorithms to match these things. So we will have a huge number of false positives if we rely very heavily on algorithms to filter.

It will of course need human intervention to analyse these false positives. So as a first step, yes, of course, you can use that, but Google and Facebook are employing 50,000 more people not as a job creation scheme and because of the benevolence of the companies but because they recognise that there will have to be a mixture in order to achieve any kind of aim.

One of the problems is that they are responding to a perceived need to remove more content, rather than addressing what you said in your previous question about fair process and due process in these things. I suspect they will focus on the former to the exclusion of the latter simply because of what I said about the Mechanical Turk idea: that they are subcontracting to people on very low wages. It is certainly not UK minimum wage; it is far below that. That is obviously a great deal cheaper than employing a lawyer to work out whether there should be an appeal to actually put this stuff back online.

I very much agree with Dr Nash about audited self-regulation, which is a form of co-regulation, being a very important element. I fear that the incentive structure that we set up will be an incentive structure for them to demonstrate how much content they have removed, when actually a very important additional question is, "Show us the examples of successful appeals to put content back online", in order to demonstrate that they are not simply, as I said earlier, shooting first and not asking questions, which would be their tendency.

Q7 **Viscount Colville of Culross:** Building on other answers you have given, I want to look at the balance that needs to be established by the platforms in ensuring online safety while protecting the rights of expression. You have spoken quite a lot about the problems with takedown notices and how that could lead to overzealous policing of content. Dr Nash talked about audits of this process. Do we leave it to the platforms to deal with the online regime, or do we need determined regulatory intervention, or even law, to make this happen? I know that you have written about this, Professor Marsden.

Also, to move on a bit further, Professor Woods, you have written about Article 10 of the Convention on Human Rights not necessarily covering various aspects of social media. Will you elaborate on that, on what we should be concerned about, and on what the remedy would be?

Professor Lorna Woods: It has just occurred to me that I should have declared that I am a member of the code committee of Impress, which is the Leveson-compliant press regulator. It had entirely slipped my mind. It is a non-remunerated post.

The common interpretation of Article 10 is focusing on the speaker. Article 10.2 gives grounds for the state to restrict speech. Takedown orders would be a prime example of that. Interference must be in the service of the public interest, it must be set down by law and it must be proportionate and necessary in a democratic society.

As for some of the problem speech, hate speech may fall outside the protection of Article 10 altogether. Article 17 of the convention—and there are analogous provisions in the EU charter and in the ICCPR—allow material that seeks to undermine the very purposes of the convention not to be protected. Very forthright political commentary may be restricted, but it has to go through the Article 10.2 analysis. Hate speech, of which Holocaust denial is a prime example, could fall outside the regime altogether.

A lot of the criminal rules we have would have to fit within that framework. That is what has led to the guidelines on prosecution and the high threshold before a prosecution will be brought for speech crimes. As I mentioned, the obligation is on the state, so if you are looking to exercise Article 10 against a private party you are looking for a higher standard. What is engaged with there is more a balancing between the interests of the party. The leading case on this is a British one called Appleby; some protesters wanted to hand out leaflets in a shopping centre and the shopping centre did not let them. They claimed that the UK had failed in its positive obligations. They lost because there were other places where they could go to hand out leaflets and make their point.

So there is a weakness there in trying to claim a right to the internet or to a particular platform. Although the European Court of Human Rights has been concerned about the impact of blocking orders—we talk about collateral censorship—it has been less convinced to find that if you are just cut off from going online to access music you have a right at all. They say that you are not even a victim in that instance. I have argued, particularly in the context of a social media platform where you are engaging with friends or family, that it may be easier to analyse it under Article 8, the right to private life, where the positive obligation seems to kick in at an earlier stage.

Professor Christopher Marsden: Very briefly on the point about comments, you may be aware that there were two conflicting judgments of the European Court of Human Rights. The first was an Estonian case, Delfi AS v Estonia—I prefer to pronounce it "Del-fie" but I am told that is not correct, and in any case it is not really a portent of the future—in which, essentially, a news website was made liable for the comments that were underneath the news article. It was fined for the comments, which of course led news websites across Europe to think that perhaps they would have to do something: either pre-moderate, which of course the BBC has always done but which commercial publishers have always said would require a great deal of investment, or alternatively remove comments altogether. That case has since been followed by a case, which I will not try to pronounce in Hungarian but is essentially MTE v. Hungary, which appears to have restored some kind of balance.

Do you want to say something about the balance?

Professor Lorna Woods: In MTE, the court approved the principles in Delfi. It just came to a different conclusion on the facts. So we are still stuck with the principles from Delfi, although differently applied in MTE.

Professor Christopher Marsden: Yes, it should be said that, without overruling Delfi, they stepped back.

Professor Lorna Woods: It was a chamber decision versus a grand chamber. Delfi was the grand chamber.

The Chairman: Thank you for the clarification.

Professor Lorna Woods: Sorry about that.

Professor Christopher Marsden: This will come back to haunt the Committee in future, I am sure.

We face a profound issue, which is that if we do require prior approval of comments, whether it be on Twitter, a news website or wherever else, we are requiring a great deal more investment, and websites may well choose to remove comment altogether. Depending on your view of comments on news websites, that may be a good or a bad thing. Let us assume that it is a bad thing to remove them altogether.

Dr Victoria Nash: Just one quick response to your other question about whether regulation is needed to balance these concerns. My view is that I would like to see how effective the proposed social media code of conduct coming out of the digital charter will be. My suspicion, given what we said at the beginning about ensuring that we do not impose high regulatory burdens that stifle competition, is that that would be the place to start. If it is not effective, we might move to a more regulatory approach.

Q8 **The Lord Bishop of Chelmsford:** I want to move us on to an area that we have touched on but have not explored much so far, which is transparency. What information should online platforms provide to users about the use of their personal data, and how should that be presented to them? With the GDPR coming in in less than a month from now, does this in your view provide sufficient protection for individuals in the use of their data, et cetera?

The Chairman: Again, I appeal to witnesses to be reasonably concise.

Professor Christopher Marsden: I shall be, partly because I work with a much greater specialist in this area, Dr Nicolo Zingales, who has just published a book called *Regulating Platforms* as a result of some United Nations work. I will share with it the Committee.

Our personal data is currently regulated from Dublin and Portarlington in Ireland; it was formerly Portarlington alone, but then it moved to Dublin and Portarlington. If you are not familiar with Portarlington, do not worry: it is a fairly small town in Ireland, but it is where the Irish Data Protection Commissioner was based. Of course, it has never fined Facebook or Google a euro. Fines are not of course the only measure of the effectiveness of statutory regulation, but you might expect something to appear as a sign of effectiveness. As things stand, we are regulated via Ireland.

As I understand, the inquiry in the other place on fake news is dealing with Cambridge Analytica, which is being examined by the Information Commissioner here, but not Facebook, which is still to be the responsibility of the Irish Data Protection Commissioner. That was confirmed by the group of data protection regulators, the Article 29 Working Party. I am somewhat cynical about trying to introduce greater transparency. The greater the transparency, the greater the amount of information you give to users, who do not read it in the first place.

On the contracts available to you—I am sure that Dr Nash can speak to this—an Oxford University study looked at how long it would take you to read the contracts that you agree to. I believe that it takes more than a year to read the contract that you go through in your first hour online. We can of course try to afford greater transparency, but the degree to which that helps us is limited. There is current controversy about the fact that Facebook has essentially relocated the jurisdiction for non-European and non-North American users of Facebook to California, rather than to Dublin, as I think many people assumed it would do. You are told that if you do not agree to the terms of service you can no longer use Facebook. That is a fairly profound response to a failure to accept what are effectively unilateral terms. Transparency is necessary, but it is a small first step towards greater co-regulation.

The Chairman: Do you agree, Professor Woods?

Professor Lorna Woods: Wholeheartedly. There is no point in giving information unless people have the time to read it, understand the ramifications and then have a realistic choice to do something different. I do not think that people do.

On the GDPR, the Facebook removal is interesting and raises the question as to where we will be with that post Brexit. As I understand the Bill, the applied GDPR takes out the extraterritoriality in the GDPR, so we will then be moved to the third country situation.

Dr Victoria Nash: Obviously, I agree with what they said.

On the question of how we can provide information more effectively about what is done with data, I have seen some interesting efforts to move to more icon-based communication. It does not tell you in great detail what is being done with your data, but it identifies whether it is being shared with third parties, for example. That is definitely a step forward. For me, the biggest problem with this, whether you write it out in full or use icon-based systems, is that it takes a great deal of time.

There is an American lawyer called Jack Balkin who, together with Jonathan Zittrain, has introduced the concept of information fiduciaries—the idea that when we are handing over data to online third parties we should be looking not for heavily detailed terms of service and descriptions of exactly how it will be used and where but more for an understanding of this as a professional relationship, where what you want to see is uses of your data that will not come back to harm you.

I know that it is getting quite late in the day, so I will not go into that in more depth, but I can send papers on it. The GDPR has some inadequacies. I am not a lawyer, but the two obvious ones for me are large assumptions about screen-based interactions, when increasingly we are moving towards internet of things devices or home assistants. Again, it is about how you communicate data use in those circumstances.

Secondly, to go back to the point made so well by Baroness Kidron, we should think about younger users and their ability to use services at an age where they are able to understand what the data transfer will mean for them. For me, those are the areas of inadequacy.

Professor Christopher Marsden: We tend far too infrequently to consider the other area of great regulatory arbitrage and changes, which is the financial services industry. One element of the Sarbanes-Oxley Act 2003, which regulates public listed companies in the United States, that should probably have been thought about more by internet lawyers was the placing of personal responsibility on directors of financial services companies to keep data safe. That changed enormously the culture around the risk management of data in financial services companies.

Giving directors personal responsibility to keep data safe or to do other things with it is a useful way of focusing attention. I know that many members of the Committee are directors of companies themselves and will be aware that that does focus the attention.

Q9 **Lord Allen of Kensington:** I declare my interests. I am chairman of Global Media & Entertainment, I am advisory chair of Moelis & Company, which is an advisory bank to media companies, and I have shareholdings in ITV.

I want to stick with transparency. In a previous inquiry, we had a social influencer who found that, although people could come to her YouTube channel, algorithms were being used to divert funds away from her. Should there be transparency in what algorithms can be used for whatever purposes and the extent to which they can be used other business models, where arguably their use could be deemed to be fraudulent? I am interested in your thoughts on those areas.

Dr Victoria Nash: My goodness, if we think it is difficult for users to understand the terms of their data use, it is impossible for them to understand how algorithms are directing their online experience. I find it hard to imagine how those might be explained in a way that would be fully transparent to users. It is a huge problem.

I can see two areas where there may be a bit more room for hope. First, it would great if we could have more algorithmic choice in the use of such services. An example would be something as simple as the chronological

Facebook newsfeed versus the items that it thinks you may most want to see. That should be an overt choice. We can imagine other alternatives, too, where you choose to highlight reliable news sources et cetera. Could we not have more overt and explicit algorithmic choice in how our feeds are organised?

Secondly, a colleague of mine, Dr Sandra Wachter, and Brent Mittelstadt are looking at how you might be able to identify examples of discrimination. That is a key thing: you may not want to understand how the algorithm works but you darn well want to know whether it has harmed you in some way. Again, I can forward more information about that approach.

The idea would be that you can use machine learning to identify the factors that seem to influence that decision: that is, you are more likely to be served this job advert if you were this, this and this. I am not convinced about transparency, but there may be other ways to address the problem.

Professor Christopher Marsden: I want to introduce use an ugly term: replicability—the ability to replicate the result that has been achieved by YouTube or whatever company is producing the algorithm.

Of course, algorithms change all the time, and one accepts that the algorithm at one particular time, for instance for Google search, is changed constantly, and there are good reasons for it wanting to keep that as a trade secret. But you would like to be able to look at the algorithm in use at the time and, as an audit function, run it back through the data and make sure you can produce the same result. We do this in medical trials all the time; it is a basic principle of scientific inquiry. It would help us to have more faith in what is otherwise a black box that we just have to trust.

I will also mention Michael Veale at UCL, who has been working with Brett, Sandra and others on this, and the idea of going beyond transparency to replicability: to be able to run the result and produce the answer that matches the answer they have. You do so independently, of course. You do not just want to ask the company, "Is that fair?", because it will say, "Yes, of course, it is fair". One wishes to do it independently.

If you can produce replicability, you can have much more faith in the system. However, companies will not just volunteer that. It is expensive for them to do, and if it is expensive to show people results it is even more expensive to show them results and make sure that they do not change your liability. They will not volunteer that.

Professor Lorna Woods: Users would need to know the purpose and effect. There is a lot of, "We can't tell you this, because it's a trade secret". I do not think that people need to know your trade secret. They need to know the principles, the purpose and how it works, although when it comes to making sure that that is actually the case, replicability and auditing are probably essential.

I question whether all algorithms are equally legitimate. There is, I think, an extremist algorithm or a phrase that is talked about in relation to YouTube and Facebook that means that when you start watching a video you are then served more and more extreme versions of the content, so your video about how to put a shelf up turns into examples of people drilling holes in their hands or something like that. I do not know whether that sort of algorithm is socially responsible, so I have a question about whether we would want to look at that.

Lord Allen of Kensington: In this particular case, she saw her commission diminish fairly substantial over a very short space of time, so she knew that there was a detrimental effect.

Professor Lorna Woods: Yes.

Lord Allen of Kensington: That was the point you were making. Thank you.

Q10 **Baroness McIntosh of Hudnall:** There are so many things that I want to ask you as well as the question that I am told I have to ask you—

The Chairman: Indeed. I think we are all in the same boat.

Baroness McIntosh of Hudnall: —but I am not going to.

Dr Nash, right at the beginning, in your opening remarks, you talked about your belief, as I understood it, that we did not need more of anything; we needed to use what we already had more effectively. My question is about the effectiveness of current competition law in renegotiating the activities of the platforms that we have been talking about, particularly given the other issue that has come up: the question of the increasing dominance of a very few of them and the aggregation of smaller start-ups into the larger platforms, which leaves the field marked very heavily by a very few, very large footprints.

First, do any of you think that current competition law is enough, if it were properly applied, to regulate the activities of these platforms?

Secondly, I think it was Dr Woods who made the point earlier about our exit from the EU and the possible deficiencies of the GDPR in relation to our status once we come out of the EU. Are there any specific risks to us post Brexit in competition regulation?

The Chairman: Shall we have Dr Nash's perspective first?

Dr Victoria Nash: You are asking the non-lawyer first. As a non-lawyer, I would not want to say too much about the efficacy of competition law except to say that to me as an outsider—a non-lawyer—it seems like the wrong hammer to crack this particular nut with. Yes, I can see that there might be inadequacies in competition law, and the whole does not take into account data monopoly, for example, or access to large sets of data across different smaller companies.

However, I am not convinced that that would resolve the sorts of problems that we have been thinking about today. Chris made a good point earlier, which is that in some ways it might serve us quite well to have very large companies that can be embarrassed in front of shareholders and Governments and which you can call to give evidence—not always successfully, I know—rather than having a very large number of small innovators who it is harder to use that sort of leverage with.

Those would be my comments, I guess. I will leave it there.

The Chairman: Professor Woods, what do the lawyers think?

Professor Lorna Woods: I guess it depends on the particular concern, but competition law does not take non-economic interests into account too well. That is why we have the public interest provisions in relation to media mergers and so on, and in order to address the problem that Chris has talked about it may be worth thinking about having a public interest test in relation to the tech start-ups—so coming in at a lower threshold—so that the privacy concerns about data monopolies could be considered in their own right and without trying to describe them in purely economic terms.

We have the example of Facebook buying WhatsApp. I think the Commission expressed concern that it could not really talk about the data protection issues, and some years down the line we find WhatsApp data going to Facebook and a lot of the data protection authorities around Europe having to take action. So there is a concern there about the non-economic aspects.

Baroness McIntosh of Hudnall: Just to be clear, you are making a distinction between competition law, which is fundamentally to do with the commercial interest, and the public interest, which is non-economic.

Professor Lorna Woods: Yes.

Baroness McIntosh of Hudnall: Are you suggesting that we already have a model that could be usefully applied, or are you saying that this happened somewhere else but you would have to invent something different in relation to these internet-based providers?

Professor Lorna Woods: I think we could look to the models that we have that sit alongside competition law in this country and that try to deal with non-economic interests. National security is one. Media plurality is another.

The problem is that you struggle to capture the value and the threats to those sorts of interests if you are using a purely economic model. It is a question of how you describe the harms and how you see the market being described. I suspect that Chris could talk more coherently about how economic thought works or does not work.

The other point is that we have network effects, which means that the value to users of the platforms is greater when more people are on them, which pushes the market to bigger providers and the market analysis is not standard. We have competition authorities in this country, so I assume that that post Brexit they would take over that role entirely.

Professor Christopher Marsden: I agree with what has been said so far: that there is this great schism between competition lawyers and communications lawyers. It should be said that I am probably a heretic when it comes to competition law; I do not believe that competition law solves the problems in these markets, first, for reasons to do with data protection, which is clearly outwith the ambit of competition law, but, secondly, because many of the monopolies that we have seen emerge in the communications agencies have emerged so fast that the claim that they are durable, permanent monopolies would normally fail the test of competition law.

So competition law will not be a solution. It is actually a wonderful way of parking the issue and saying that we do not have to deal with it. We will come back in 10 years' time and see where Facebook is, and who knows where we will be in relation to Facebook at that point. That is one issue that emerges.

The other issue is Brexit. I have not mentioned the B word so far, but a lot of people in the industry were surprised to learn that we will be leaving the Digital Single Market post Brexit. That is quite a dramatic step for the UK communications industry to take. If we do, of course, we become a rule taker from Brussels across this set of issues. One reason why people in Georgetown and other places look at us and say, "How do you solve the problem?", is because we were always considered to be problem solvers in Brussels in Digital Single Market issues.

Leaving aside the cliché of the unsinkable aircraft carrier and the fact that the American companies have huge investments in the UK, the assumption was that we would temper somewhat the views in Brussels that were taken by the other major party—the German-French alliance—on some of these issues. That ability to influence Brussels substantially disappears if and when we Brexit. As a third country, it will be very interesting to see the extent to which we can influence the regulation of platforms.

Brexit opens up new opportunities. I think the Secretary of State has suggested that, for the first time in a very long time, we can rewrite the Electronic Commerce Directive, which terrified almost everyone I have spoken to about it. That really is untying a Gordian knot. It will be very interesting to see what happens. We will be in a very different environment, and while I assume that the Committee will only be able to be very prospective in its discussion about what will happen post Brexit, it means that some of our stable understandings about the intervention of competition law and other things will change very rapidly.

The Chairman: We have only a few minutes left, but you are introduced to our next question. Baroness Bonham-Carter was going to ask about the effects of leaving the European Union. It is at the heart of all public policy at the moment. Would either of the other witnesses like to address that?

Professor Lorna Woods: I suppose there is the Schrems point, if we are talking about data flows, which is that as we move out of the single market we will have to prove that our data protection standards are adequate from the perspective of the EU. There was a rather famous—to lawyers—case called Schrems, in which data flows to the United States were challenged on account of national security surveillance powers. At the moment, we do not have to justify our regime; we are presumed to comply. We will not get the benefit of that doubt once we have exited. One of the big questions that will affect this area is going to be data flows.

The Chairman: Dr Nash, what does Brexit mean to you?

Dr Victoria Nash: I would add that it is not just data flows but data rights for UK citizens, given that we do not have as great a record on preserving those data rights as might have been wished.

Professor Christopher Marsden: There is another point—it might seem very minor, but it is the area I am best known for—which is that we have an Open Internet Regulation. That introduced, first, pan-European mobile roaming, which some of us enjoy. I suppose if we do not leave the country, we do not worry about that disappearing afterwards. The second thing is the net neutrality rules, which are in a state of some flux at the moment. I sit on the advisory panel for a report on the implementation of these rules in Brussels.

A certain problem that will emerge if and when we leave the European Union is that we will no longer be required to follow those rules on, for example, zero rating. One aspect of that that the Committee might be interested in is that when you look at mobile phone contracts in the UK at the moment, many have zero-rating on specific applications—Spotify, for example, and even Netflix, which are very large consumers of data. Most of those do not—none does, as far as I am aware—include the BBC, as a non-commercial player. There is no incentive to allow iPlayer data to be consumed freely in that way.

It will be interesting to see whether there is a divergence in the way the net neutrality rules are implemented. If you invite Ofcom to give evidence, it might be able to say something about that, because Ofcom wrote the rules that we have in Europe. It was the chair of the working party of the body of European regulators in the area. It would be interesting to see, having written the rules, if we then go outside the rules, the extent to which we conform to the rules.

Q11 **Baroness Kidron:** My question comes in two parts. Listening very carefully, you say when directors in the financial services became responsible, suddenly their normal behaviour got a bit better. That seems like an argument for regulation rather than no regulation. I thought that the points around transparency were very interesting, but when Facebook get a choice they move out of Ireland and into California. I am just curious: is your fear a fear of bad regulation rather than regulation? Please be brief, because I then want to ask just one thing about the international picture.

Dr Victoria Nash: Clearly, I fear bad regulation much more than I fear regulation, but I guess that I want to see evidence of a clear problem that regulation can solve.

Professor Lorna Woods: I suppose nobody wants bad regulation. I am less worried than Dr Nash about the problems that regulation might bring. We have a long history of various forms of regulation of various forms of public communication. We seem to come up with a balance, so it is possible and we should try.

Professor Christopher Marsden: One reason why we constructed the Beaufort scale, with these 12 degrees of co-regulation, is in order to be able to move sectoral regulation up and down the scale according to conditions in society and in the market. That may be a more flexible way. One of the advantages of co-regulation is that the Government can always blame the market for not producing the results they want. They say, "We were not regulating, so it is not our failure". It is the market's failure or the user's failure, even.

Baroness Kidron: Obviously this is a global issue, and it is an international set of agreements that we all ultimately need. Is there a natural place where that should come from? What role do you think the UK could take in trying to establish something at a global level?

Professor Christopher Marsden: Is this the post-Brexit question?

Baroness Kidron: Irrespective, actually.

The Chairman: Inevitably, it is.

Professor Christopher Marsden: I declare an interest in that I have consulted for the Organisation for Economic Co-operation and Development over the last two years on regulation in this area.

Mexico at the time was the largest non-European member of the OECD, aside from the obvious United States. In terms of size of economy, we will become the largest non-aligned member of the OECD post Brexit. The OECD does some fascinating and important work in this area—not direct regulatory work but work that helps to advise on regulation—and I suggest that some of its work has been very influential in assessing what we should do about intermediary liability, for instance. It is a really interesting venue to consider the evidence from. A lot of it is statistical evidence.

The other area is the United Nations Internet Governance Forum (IGF), which apparently will happen this year. Apologies. I am addressing a member of the millennium broadband commission, so I will not perhaps continue on that. You are aware that the United Nations does work in this area because you are doing that work. Forgive me.

The Chairman: Not necessarily all of the Committee is.

Professor Lorna Woods: There are a number of bodies that you could say have an interest. If we are talking about the UN, there is the ITU—the International Telecommunication Union. That is quite a difficult place to get agreements, so I am not sure that I would like to see that body taking up the reins for more content-end stuff. It has a long history on infrastructure and technical standards, although to some extent it is being superseded by the Internet Engineering Task Force, the IETF.

I suppose the problem is that once you get to global levels you are actually dealing with a lot of different perspectives about what is important, what is good and what is necessary. It becomes hugely difficult to get agreement, except at a level of very general abstract principle.

Sometimes some of the documents that come out are actually internally contradictory; you have a statement about the importance of freedom of expression and the next statement is about the importance of somebody’s reputation. I am not sure how far they would really take us. There are some bodies that can do technical stuff quite well, which is important for the practical functioning of the internet, but if you are starting to look at content standards, it is very difficult to get agreement on that. Then, implementation comes down to the nation state.

Dr Victoria Nash: The main function of international organisations in the regulation of the internet is to provide spaces for a variety of different stakeholders to have a say in the governance of the internet, not just nation states. We have mentioned the ITU. UN bodies are more nation-state focused, as you said. It is very difficult to get state-level agreement on these issues. For that very reason, some of the most important ones are those that do not have direct decision-making power, such as the IGF, the IETF and ICAN.

There is also increasingly a space for newer types of international body, which may have a small slice of the pie. The Global Network Initiative, for example, is really interesting and helps to speak to this idea of agreeing international norms or standards to which internationally operating companies that want to abide by it might be held accountable. Again, I do not think that there is a role for the UK Government there, but there is a role for UK citizens and other bodies.

The Chairman: I thank our witnesses for their very comprehensive evidence. The Committee hugely respects expertise and experts and we have a voracious appetite for evidence. You have given us plenty of both and we really appreciate you taking so much time to give us our first set of evidence for this important inquiry. You have also promised us quite a reading list of material. The clerk has written most of it down, but we would appreciate it if you sent us all the reports and written material that you referred to.

Thank you again for joining us and for speaking in English, by the way. It is quite hard for experts always to communicate in clear English, and you all did that very well.

Match Group and Twitter – oral evidence (QQ 122-127)

Tuesday 11 September 2018

Watch the meeting

Members present: Lord Gilbert of Panteg (Chairman); Lord Allen of Kensington; Baroness Bertin; Baroness Benjamin; Baroness Bonham-Carter of Yarnbury; The Lord Bishop of Chelmsford; Lord Goodlad; Lord Gordon of Strathblane.

Evidence Session No. 14 Heard in Public Questions 122 - 127

Examination of witnesses

Jared Sine, General Counsel & Secretary, Match Group (via videolink); Nick Pickles, Senior Strategist, Public Policy, Twitter.

Q122 **The Chairman:** Welcome to our second evidence session this afternoon on our inquiry into the regulation of the internet. We have two witnesses. On the screen, we have Jared Sine, who is general counsel and secretary for Match Group. Thank you very much for joining us, Mr Sine. In a moment we will ask you to say a few words by way of introduction. Our second witness is Nick Pickles, who is the senior public policy strategist for Twitter. Welcome both of you and thank you very much indeed for coming to give evidence to our inquiry. The session will be recorded and a transcript will be taken.

May I ask our witnesses to say a word of introduction and, in so doing, perhaps answer our opening question, which is: has the internet outgrown the regulatory model of self-regulation and co-regulation? Mr Sine, can we start with you with a few words of introduction and a brief answer to the question?

Jared Sine: Sure, I would be happy to. First, I want to thank you, my Lord Chairman and the committee, for the opportunity to present evidence today. Before I proceed with answering the question, I would like to provide a brief introduction to Match Group as well as myself. As was mentioned, I am the general counsel for Match Group and, first and foremost, I want to apologise for not being able to join you in person. I would have loved to be in London at this time of year. Unfortunately, I am unable to do so, but I appreciate your willingness to allow me to join by VTC.

While we may not be the largest of the players that you have spoken with, we believe that as a small to medium-sized platform we offer a unique perspective that should, hopefully, prove informative in connection with your inquiry. It is for that reason we felt it was really important to have someone from our global leadership team join this discussion today.

In terms of who Match Group is, we are an operator of leading online dating brands across the globe, including Match, Tinder, PlentyOfFish, OKCupid and others. We do not take our position as a leader in this category lightly, which is why we strongly agree that public trust in the digital economy is essential and good for all of us. It is for that reason that we support reasonable legislation and regulation in this area, to the extent that it is carefully and thoughtfully crafted, with the input of industry players. One of the reasons for that is because our business model breaks with the traditional business model of online platforms, where platforms effectively offer a free service which is subsidised by the use, sale, monetisation or other licensure of data. Instead, the overwhelming majority of our revenue is derived from subscription services for which our users pay. So already as part of our business model and culture, it is essential that we offer an enjoyable user experience, and one that is safe and engaging for our users, because if we do not, our users will not come back and they will not continue to subscribe, and that would have negative impacts not only on our business model but also on our community at large. As a result, we are constantly innovating and rolling out new feature sets, products, et cetera, to try to ensure that our users have a safe and enjoyable experience on our platforms. In fact, 10% of our workforce is dedicated to safety and moderation efforts.

In terms of your question as it relates to has the internet outgrown the regulation that exists today. As we all know, the internet has grown rapidly and has now penetrated most every aspect of users' lives. Phones are ubiquitous, online access is ubiquitous and the regulation has, in some respects, lagged behind, which is again why we support regulation or legislation that is consistent with the different needs of the various platforms.

One thing we are concerned about as it relates to regulation is a one-size-fits-all approach that is rigid and targeted at policing and regulating the largest online players. As I mentioned, given the fact that our business model breaks from the business models that are traditionally out there in the online world, it is important that these differences are taken into account, and that any such legislation or regulation is flexible and provides us with the ability to craft solutions to the specific needs and issues that our businesses face.

We also think it is important that as regulation is developed, it is done so in a way that takes into account the various concerns that businesses such as ours have in terms of making sure that the balance of power between various laws and legal regimes is taken into account in connection with such new legislation. For example, in many of our platforms we would love to make further or greater use of automated scanning and other tools that would allow us to review content posted to our platforms, including private messages and other content, to the extent that it contains harmful, offensive or bad behaviour, but, unfortunately, there are a number of privacy law regimes that would restrict our ability to do so. While we would not want access to do so carte blanche, we think that having access and making sure that these regulatory regimes take into account these existing restrictions is critical to ensuring that, to the extent there is new regulation developed, it is easy to adopt and deploy.

We think it also makes sense that any regime adopted or deployed does not end up further shifting the balance of power into the largest players' hands at the expense of the smaller players, given the fact that we have more limited resources and we have constraints along those lines.

Ultimately, I think that what is most important is that as regulation is thought through and crafted, industry plays a key role in that, so the differences that the various platforms and businesses face can be taken into account in connection with that regulation.

The Chairman: Thank you. Mr Pickles, could we have a word of introduction from you, please, and your thoughts on whether or not the internet has outgrown the current regulatory regimes?

Nick Pickles: Thank you for the opportunity to appear today. It is a change for me to appear alongside a video camera. This is an incredibly timely inquiry given the public policy conversations we are having around the world. Previously at Twitter, I spent four years based in London leading the company's public policy work in the UK. I now live and work in San Francisco. My role as a senior strategist is to try to bring together the public policy debates we are having around the world on issues such as terrorism, safety and abuse, disinformation and election integrity, and to bring together the views of our product teams and the Trust & Safety Council, which enforces our rules and writes our policies, to make sure that we try to understand different perspectives when we makes decisions as a company. You may have seen our chief executive testify to Congress last week. We have to be very mindful that the decisions we make have great impacts. We are companies that have real impact in the real world and we need to think carefully, and perhaps in the past we have not thought carefully enough about how we take steps to ensure the health of the conversation that is happening.

The interesting aspect for me when we think about internet regulation is that we often jump straight into the regulation of companies and we miss the regulation of the internet itself. The current challenge in the developing multi-stakeholder model of international internet governance is critical. This is how countries come together through a sea of acronyms, across ICANN, the ITU and the IGF. The reason this multi-stakeholder model is very important is that it has normalised the idea that states cannot control the internet. That means we have a global, free, open internet where information can move across boundaries and borders without states having undue control of that information and the undue restriction of free expression, the erosion of privacy and government censorship. That multi-stakeholder model is far more fragile than people realise. There are concerted efforts from countries around the world that do not share our values to try to get to this state-based internet.

A challenge when looking at national legislation and regulation—and the Information Commissioner illustrated well the existing full spectrum of different laws that apply to companies such as Twitter—is: how can you make sure that something that happens in the UK does not have an effect internationally that changes this very delicate balance? The internet has evolved, driven by free expression, and many services such as ours and the web generally have been driven by self-expression and user-generated content. A lot of the conversations we are going to have today go to the heart of user-generated content, which is people speaking, and are as much constitutional ones as they are commercial, because at the heart of this we are talking about regulating speech. It goes back to the Information Commissioner's analysis of trying to understand what specific harms we are trying to address, what the policy objective is and what the best way to get there is. One week I am focused on issues around elections and the next week I might be looking at aspects of terrorism. The problems and the solutions are very different. Some are local and some are international and some are between industry and self-regulation.

A real risk we face now is a result of the huge successes that have happened online. The UK has the highest proportion of digital economy of any G20 country and that is as a direct result of the UK's regulatory framework. At the same time, the Internet Watch Foundation, a remarkable organisation that seeks to remove child exploitation material from the internet, over the past 20 years has reduced the amount of that content hosted in the UK to about 0.3%. It has been tremendously successful in doing that and that is an industry-led and funded body. It is interesting that in its work it finds only about 1% of the content on social media; the rest is elsewhere on the internet.

Today I am looking forward to discussing this notion whereby we sometimes confuse the internet with half a dozen companies, many of which appear quite regularly before Select Committees. The ecosystem is far more diverse and complex. It is a welcome opportunity to have that more complex discussion today.

The Chairman: May I ask our witnesses to keep their answers to questions reasonably concise, as we have quite a lot to get through and we would like an opportunity for discussion with members of the committee?

Lord Gordon of Strathblane: To take a specific example, is there a danger of a conflict between British and American law? In written evidence it was alleged—and I put clearly that it was only alleged—that Twitter had refused to enforce a UK court order without a similar order from an American court. Is that the case?

Nick Pickles: I am not familiar with the specifics of that case but I will happily follow up on it. Absolutely, there are situations where companies find themselves in positions where two different legal jurisdictions will impose different legal obligations. Industry and the UK Government have worked a lot in recent years on situations where UK law enforcement agencies require information that is held by an American telecommunications company—Twitter, Facebook, others—which US law would preclude us from disclosing and where it would be illegal to do something in the UK that is being requested by UK law enforcement agencies. Recently, the CLOUD Act has been passed by Congress and that is specifically to solve this problem between two jurisdictions and, as the Information Commissioner mentioned, will be underpinned by a bilateral agreement between the UK and the US. I will look at the specifics, but we have to be honest and say that one of the big challenges we have as companies is that the overlap of government-to-government legal frameworks is not always easy.

Lord Gordon of Strathblane: I see Mr Sine nodding in agreement. Do you wish to add anything to that answer?

Jared Sine: I would echo the sentiments. I think it can be very difficult for multinational corporations, whether it is Twitter, whether it's Match Group, et cetera, to make sure that all of our policies and approaches comply with the various legal regimes out there. Unfortunately, there are situations, as previously described, that create these conflicts. We do our very best to address them. The MLAT procedures that used to exist to help facilitate the transfer of data across country lines into the EU, which we would work with EU law enforcement and others who required information in connection with investigations, but it can make it very difficult, for sure.

Q123 **The Lord Bishop of Chelmsford:** My question, perhaps to you first Mr Sine, is: to what extent should online platforms be liable for the content they host? To add to that, should the liability obligation differ between platforms according to their size or function?

Jared Sine: I believe that platforms should have some responsibility to ensure that they are monitoring and reviewing the content that is on their platforms, but I do believe we have to be very thoughtful in how we craft that liability regime. The reason I say that is, all too often what happens is liability regimes are crafted in such a way that those who don't monitor or make proactive efforts are actually rewarded in some respects because their lack of knowledge as a result does not impute any kind of liability to them , whereas platforms who are proactively doing the right thing and trying to bring down offensive or inappropriate content are actually held to a higher standard because they are proactively monitoring and reviewing. In that respect, I do believe platforms should be working to monitor, to review, to actively take down content, to the extent that it is reported to them. But in terms of the liability, I do believe there should be good Samaritan or good faith effort-type provisions that allow organisations that are doing the right thing to avoid liability to the extent that, in connection with their efforts, unlawful or inappropriate content slips through cracks of the nets that are established to try to identify that content.

The Lord Bishop of Chelmsford: I will give Mr Pickles an opportunity to answer the same question, but why should the onus be on taking down; why not on not putting up?

Jared Sine: Let us look at our platforms for instance. If you look at the Match Group platforms, we differ quite dramatically from many of the other online platforms. While we do have an area where information is publicly posted—for instance, a person who is looking to find a date or a significant other will post their information in a profile—most of the communication that happens on our platform happens in one-to-one private messaging, and so to the extent you were to require businesses to scan that information prior to it going on to the platform, you would unnecessarily be delaying the ability of users to interact with one another, artificially changing and altering the normal behaviour that people would otherwise engage in and pushing them into platforms that we cannot monitor or help to provide our services on, such as cell phones or other messaging communication tools such as Snapchat, et cetera.

So in terms of creating a system where content is reviewed before it goes up, it would really hamper the experience for the users and the effectiveness of the systems and the tools and the services that we are trying to offer. We do have a number of tools and systems where we scan profiles and other things, on certain of our platforms, as they are coming up, and, on certain of our platforms, very shortly after they come up. We believe we have tools and systems that quickly identify this type of behaviour, but I do believe you would materially alter the services and the efficacy of the business models that are out there online if suddenly there were this up-front moderation that had to take place before any content could be posted to our platforms.

The Lord Bishop of Chelmsford: I may want to come back but of course I know there may not be time. If I have heard you correctly, that could be something to do with the function of the different platforms, so perhaps we should hear Mr Pickles' views on this one, because Twitter is a very different sort of platform to Match.

Nick Pickles: I think that the rich variety of different services is a point to remember as you are exploring this issue. Twitter has 35 million users around the world, which sounds very large, but in terms of our peer companies, which may have several billion users using multiple services, in some calculations we are quite small. A real challenge with this issue of liability is that—and this is perhaps my Yorkshireman's scepticism coming through—floated very regularly as the solution to every problem in every shape is to flick this liability switch and all these problems will go away. The Yorkshireman in me says, "Be suspicious of someone who promises you a simple solution because the likelihood is it is far more complex than that".

It is a question, as the Information Commissioner mentioned, of whether we are talking about illegal content liability, because if you look at things such as Twitter, for example, and the steps that industry has taken around terrorist content, establishing the Global Internet Forum to Counter Terrorism to combat terrorist use of the internet, less than 0.2% of the terrorist content we remove is reported by Governments. We detect the overwhelming majority ourselves. We remove some 75% of the accounts and we take them down before they have tweeted. Again, in the case of illegal content involving child sexual exploitation, a tiny fraction is on social media because social media companies are proactive in addressing the removal of it. Last week, the Home Secretary mentioned in his speech how in one year the National Crime Agency received more than 80,000 pieces of information to assist them to prosecute people.

Baroness Bertin: He also said that you guys had to do more.

Nick Pickles: The interesting point here again is the word "industry". I am speaking on behalf of Twitter, a company which is relatively mature in this space now and has been party to government conversations, is a member of the Internet Watch Foundation and has worked with the National Center for Missing and Exploited Children in the US for many years, and has resources dedicated to fighting this problem. One of the challenges when we talk about industry is that we are talking about the fact that the Metropolitan Police is currently working with more than 300 platforms to request the removal of terrorist content, when, often, the problem is framed as being one that affects a small number of companies.

To the upload point, a challenge there is that the significant resource constraints on small platforms to do that would have a competitive impact on them.

The Lord Bishop of Chelmsford: Out of interest and as a footnote, do you consider the term "platform" to be an adequate descriptor of who you are? I have to say as a user I find it woefully inadequate. I do not experience you as a platform, not least because of all the adverts you send me. Do you yourself think that is an adequate way of describing yourselves?

Nick Pickles: It is a really good question. One of the challenges in this space is we do not even have the language for some of these things. People try to flit between existing norms and frameworks and putting Match and Twitter in the same bucket is quite challenging in itself. This goes back to what the Information Commissioner was saying, in that perhaps we are approaching this the wrong way. Rather than looking at the internet and platforms as an entire body, we should focus on the specific policy harm. If you take terrorist content, what we see there is challenging because, as the larger companies have dedicated resources to removing the content, it has splintered across the internet into companies based in countries that do not have legal relationships with the UK and that do not engage with law enforcement. It has splintered in a way which was perhaps unintended and unexpected. How you solve that problem now looks very different from how it did three years ago, when there was more of it on the larger platforms. We have taken self-regulatory steps to tackle that problem, and I think we have made real progress. Moira Conway at Dublin University has done a lot of work looking at how the Daesh community have moved and been displaced, and we are very proud of that. It poses a different policy challenge and I think that is not quite there.

The Lord Bishop of Chelmsford: I recognise and acknowledge what you and others have done when it comes to illegal content, but by continuing to define yourself as a platform and therefore a neutral space upon which others stand, it feels to me like it could let you off the hook as regards harmful addictive content which is not necessarily illegal. To use an example from another world, supermarkets have been told, "Don't put the sweets by the checkout because that is harmful for children's health and well-being", but you do still put the sweets by the checkout.

Nick Pickles: One of the challenges of internet policy is that you sometimes have to stretch metaphors somewhat and I am not sure what the sweets are on Twitter, given that you choose to follow an account, you engage with content that you choose to consume and it does not have a calorific value that has a direct read-across to health in that sense. The question mark comes whereby we have rules that cover a broad range of activity. We face a challenge of enforcing our rules in a way that is neutral. You may have seen in the US we have been criticised for applying our rules in a biased way to favour different political groups, and we have been very direct in saying that is categorically not the case. How we enforce our rules is a challenge. The Information Commissioner used the word "trust" and long term, for us, our users trusting our platform is about making sure that the experience they have is healthy and the conversation on Twitter is healthy. That is why we talk a lot about health. It is slightly abstract, but we think there is a different way of looking at content than just: is this tweet good; is this tweet is bad? Context is everything and a tweet can be good in one context and bad in another. We are looking at the health of the conversation across the platform, and are working with the University of Oxford as well as a group led by Leiden University to try to come up with a way of measuring this, because we think there is a longer-term benefit. We see this as not a Twitter-specific issue but as a "health of the public" conversation. We are there to serve that and we hope to share the work we are doing with the whole of industry, so we can try to improve the health of the conversation across the internet and not just one company.

The Lord Bishop of Chelmsford: The Chair is going to shut me up at any moment, but finally and briefly, to give Mr Sine a chance to comment again, since it appeared you would open to thinking of some new language which might be more helpful philosophically in thinking about these new worlds we are in, would you like to think aloud as to what a good word might be other than "platform"?

Nick Pickles: It is a conversation. Industry has to be honest here. This is a conversation we are having as well.

The Lord Bishop of Chelmsford: Would you like us to come up with one?

Nick Pickles: This is where the opportunity is to have a dialogue. I live in San Francisco but I can get on a video conference. We need to have suggestions. Industry is thinking about this, as are academics, and Demos has done some great work on this. One challenge is that we are not going to solve the underlying policy issues around harassment or terrorism by focusing on the definition of the companies involved. Sometimes we put the definitions and the regulatory framework first and it detracts from us saying, "How do we solve this very hard policy question?" Some of that is regulation, a lot of which is already in place, some of it is self-regulation and some of it is societal. One thing that has really struck me in my four and a half to five years working in industry is the belief that you can solve a social challenge by removing content or removing it from particular platforms that are more visible. That is a mind-set that we need to challenge.

The Chairman: Mr Sine, do you have anything to add having had a little more notice of the question?

Jared Sine: In terms of definitions, again, we have used the term "platform" relatively loosely. They are all online services intended to achieve an outcome for the various users. If you look at Twitter, it is a forum for users to have open discussions and dialogues. If you look at our services, they are uniquely structured for users who are 18 years old and older to engage in meaningful relationships and discussions individually and privately. I do not know that we necessarily solve the problem by changing the terminology from "platforms" to "online services". The key issue remains that while we are online, we are all in many respects doing things very differently at times and other things the same, by virtue of the fact that we are online. I do think that is where the challenge is going to be for additional regulation. Mr Pickles' idea of, essentially, focusing on the policies and the social harms that we are trying to address is the appropriate way to try to think about it and look at it because, for instance, in terms of offensive content on our platform, the offensive content usually happens between two users during a conversation. We take that seriously. We have a zero-tolerance policy and we remove users to the extent that they are using offensive, illegal or otherwise inappropriate behaviour, whether on or off our platforms, to the extent we can identify it. To legislate for that would be very difficult because you would have to define each type of offensive or inappropriate behaviour. The way to think about it does have to be broader, as Mr Pickles suggests.

The other thing to think about is we work very hard to remove inappropriate content from our platforms; we are by no means perfect at doing it, and there are things that slip through the cracks. However, it is a broader societal question of how do we help society to understand that just because you are online and just because you are potentially hiding behind anonymity, you cannot say whatever you want to say. There are things that I think platforms can do but I also think that there are things that society at large needs to focus on.

Baroness Benjamin: Many young people say they steer away from Twitter because the message is in your face and you do not have a choice whether you want to see it or not, unlike other platforms. Do you think there should be some sort of mechanism for the consumer to decide whether they want to see a message or not? I know on my Twitter account if there is a message I do not want to see, I can block it. Do you think there should be a better mechanism developed so you have a choice as a consumer whether you say, "Yes, I want to see this"—whether it is sexual, abusive or porn, whatever it is; I have as a choice whether I want to see it or not?

Nick Pickles: The committee talked about algorithms in the last session. It is not good enough for industry to make decisions for users. We need to give users more controls that they own themselves. At the heart of Twitter you have the choice of whom you follow. You start with a blank timeline and fill it with people. When I joined the company, if someone replied to you, the only thing you could do was block them. There were no tools, filters or controls. We have rolled out a wide range now so you can say, for example, "Don't show me tweets that include certain words". That is often used by people who do not want to see who has won "The Great British Bake Off", and they mute #bakeoff for a week while they are on holiday. That also allows you to say, "Do you know what, I've had enough of the Brexit conversation. I don't want to see tweets about Brexit", and you can mute that word. We have rolled out a set of filters that allow people to say, "Don't show me an account if someone hasn't confirmed they have a phone number", and they are using the phone number of their phone—that is a new account; maybe someone who has not changed their profile picture; the brand-new accounts that just tweet at people. By putting controls on to users, we think we can help tackle this. One of the hardest questions in this space centres on the fact that many of the issues are subjective. Trying to write a rule about something that is offensive is very difficult because different people find different things offensive. Where it crosses the line and breaks our rules we want to remove it but where the content does not break our rules, I think you are absolutely right, companies should be doing more. Rather than saying, "The algorithm will sort it out", they should say, "Here are the controls that you yourself can use". On Twitter on the home timeline you can choose to turn on or off the algorithm that orders the tweets, so if you want to not have a certain set of tweets shown first, you can turn that off.

The Chairman: You are saying that you develop personal algorithms where as a user I own the algorithm and it is a slave to me rather than to you.

Nick Pickles: Yes, and I think that is one of the things our CEO has been talking about a lot; giving users much more control by using new tools so that you can control your experience and the order in which you see things. By keeping those controls present, rather than just saying we will take the controller and let the algorithm work, we think that builds trust, because if you do not trust the algorithm you can turn it off and see what happens. Those are switches now in your Twitter profile that you can go and look at. As a company we are looking to build much more in the future is that user control to allow you to make sure the choices you make about what you see are the choices for you.

The Chairman: I think we will move on. Lord Gordon.

Q124 **Lord Gordon of Strathblane:** Staying with Mr Sine, both of you have indicated in the last answer some measures you would take to improve the service you offer what you regard as your communities, even if they are global communities rather than small local ones. Are there any other aspects of the way you try to safeguard and maintain community standards online?

Jared Sine: Sorry, could you repeat the last part of that question? My apologies, the line was a bit garbled.

Lord Gordon of Strathblane: I was recognising that you have already given part of the answer in your previous answer, but how do you establish and maintain community standards for content and for behaviour?

Jared Sine: The way we establish the standards for our community is we first look at the legal requirements that are out there: what is legal, what is lawful content, et cetera. We then take it a step further and try to look at the experience that our users would want to have on our platform. Do they want to be bombarded with solicitations? Do they want to have people treat them rudely or inappropriately? We look at the environment that people would want to operate in and then we try to build our community standards off the back of that. We also make sure that our users agree to those community standards up front. The reason that is important is because then if users violate those standards, we are able to remove them from the platform, to ensure that in that community environment, safe and enjoyable experience, is able to be had by our users. It gets a little grey in our world given the fact these are adults and they are talking often times about intimate things, and what is offensive to one person may not be offensive to another. We try to take a very uniform approach to try to address those types of issues. If somebody is reported multiple times for behaviour that they might think is okay but multiple users think is offensive, we take that into account as well as our community standards. It is a bit of a difficult area for us to operate in given the fact there is not a lot that can be done from a legal standpoint to define what is inappropriate versus appropriate content as it relates to two people trying to engage in a dating relationship.

Lord Gordon of Strathblane: You raised one specific point and mentioned you are different from a normal internet company in that you do not use people's data. Equally, you must accumulate a vast amount of data on every subscriber you have. Do you do anything with that data? Do you make it available to any other parties?

Jared Sine: We use that data solely to provide our services. We have third parties who help provide our services. For instance, we have relationships with companies such as AWS, to provide technology services, et cetera, to help us offer our solutions on a global basis, but in terms of actual sale or licensure of that data we do none of that. We do use some limited data in terms of advertising on our platforms, but to put that into perspective, it makes up well less than 5% of our total revenue. Again, the vast majority of our service is focused and dedicated on using the data that you provide us to ensure that you have the best experience on our platform, not that that data goes to other platforms.

Lord Gordon of Strathblane: Turning to Mr Pickles, is that what you would like Twitter to do?

Nick Pickles: The first thing is to recognise that it is never static. Sadly, people are very creative sometimes when it comes to being unpleasant to other people. We try to look at what is happening and keep one step ahead of those bad actors. One of the challenges is we change the rules, the bad actors change their behaviour to try to get around the rules, and we are constantly evolving. We established a Trust & Safety Council which brings in safety expert groups and academics from around the world, not just the US and the UK but groups from Korea, Latin America and the Middle East, who share with us, "These are the trends and the challenges we are seeing; how can you make sure your rules are staying ahead of it?"

I would give you one very specific example of the upskirting Bill, which was being discussed in Parliament recently. We wrote our policy some time ago for what has become known as revenge porn, but rather than restricting it to revenge porn, we framed the policy as being non-consensual intimate imagery, which meant that our policy already covered over types of content. Sometimes very specific policy changes are unhelpful because they remove the flexibility to act in other areas. Our Trust & Safety Council is very important. We work with academics and non-profits who are working on these issues, as well as users. Anyone who has used Twitter and seen a new feature being rolled out will know that our users are very vocal in telling us what they think of our changes. There have been occasions where our users have responded and we have undone changes that we have made.

Lord Gordon of Strathblane: Is the very creation of your job which you have taken up over the last few months a recognition by Twitter that it has not been doing enough in this field in the past?

Nick Pickles: Without recreating my job interview, we have a team of 40 public policy people working around the world. Some of those are regional jobs and some are global jobs. Where my role is adding value, hopefully, is in this connection between product and policy and public policy, in that any large organisation always has issues around how it gets different teams to work together and I am, hopefully, bringing different insights to my colleagues in San Francisco. You heard from the Information Commissioner on GDPR and sometimes it is just making sure that people understand what is happening and being that connective tissue. I hope that I am adding value to my colleagues in that endeavour.

Lord Gordon of Strathblane: What processes do you use to ensure that user complaints are dealt with fairly? In a way, that means that the messenger must be identifiable. Is there anything we can do about making sure that only people who have a recognisable address and some method for putting right what they have done wrong are allowed on Twitter? Is there anything you can do?

Nick Pickles: As I mentioned earlier—and the optimist in me likes to remind people—only about 1% of Twitter accounts ever get reported for breaking our rules. The overwhelming majority of Twitter users do not break our rules and do not abuse. We see people using Twitter from other countries, and there was an academic study from Mexico a few months ago which spoke about how the public have higher trust in journalists who do not use their real name when talking about drug cartels because of the physical danger that that job puts them in, so they feel by using their real identity they must not be doing their jobs properly. I have been privileged enough to meet people who practise religions or have political viewpoints that are illegal in some countries and they use Twitter without using their real name to communicate with the world. The ability to be pseudonymous and to not have your real name and real identity on the internet is an important part of enabling free expression. However, we will take action if you break our rules, irrespective of whether you are using your real name or not. We have introduced a system whereby if you break our rules we might challenge you, a bit like a speed awareness course: "You have broken our rules. Here's the tweet. Before you can come back on Twitter we are going to give you a timeout. You have to stay off the platform for 12 hours or seven days and you have to confirm your phone number so that we know there is a connection between you and your Twitter account". We have seen that a lot people who get put through that process once do not break our rules again. We think we can improve behaviour and allow people to have their own creative choice about the identity they use online.

Lord Gordon of Strathblane: I am tempted to react by saying that hard cases make bad law. For every case where anonymity is necessary for self-protection, there are, I am sure, dozens where it is simply an abuse.

Nick Pickles: We remove those accounts if they break our rules. We co-operate with law enforcement agencies around the world to investigate those things. There have been court cases in the UK where people have abused people and been prosecuted for it, which is the right thing to do, to hold those people to account. We remove accounts. Law enforcement agencies prosecute people. We think that is the right balance. That should not be at the expense of someone who needs pseudonymity to express themselves.

Baroness Bertin: May I follow up on one point you mentioned earlier, Mr Sine, about being over 18? Age verification strikes me as still a very big problem with Twitter, and, presumably, with Match.com and other more adult content platforms. Could you comment on that very briefly?

Jared Sine: I agree that one of the challenges that all internet companies have is verification of age and identity. We all work hard to try to come up with the best tools and systems in order to do that. Unfortunately, the infrastructure globally is not in place where it is easy to be able to identify and to verify all these things, but we do employ a network of tools and systems to try to make sure that, in the event that anyone who is under the age of 18 tries to get on our platform, they are either blocked or removed very quickly. We start that process by first requiring the user to enter their actual birth date. Of course, a user could add an incorrect birth date and lie about their age. If they do, we have a series of automated as well as manual tools such as photo review, profile review and, in certain instances where it is allowed pursuant to the privacy laws of that country, message review to ensure that we can identify and remove any users who should somehow slip through the cracks who are under the age of 18. It is definitely a challenge that we face. We find in our platforms that are based in the EU, far less than 1% of the accounts created—0.13% of the accounts created—are by underage users and they are removed very quickly thereafter. We grapple with and work hard to try to address that.

Baroness Bertin: We are running out of time.

Nick Pickles: There is a tension, as we have heard from the Information Commissioner, between the objective of reducing the collection of personal data by companies and trying to verify age and identity by using things such as passports and ID cards. Twitter is a service that is overwhelmingly used by older people so we do not see a huge amount of that. Ofcom data looks at that.

The issue around age verification and verifying identity depends on whether people have passports or government ID.

Baroness Bertin: If you are an off-licence owner, you are breaking the law if you sell alcohol to children, for example. Should the onus not be put on the companies to make sure they are absolutely not allowing children on to their sites?

Nick Pickles: Are we talking about 18 year-olds, because in the case of alcohol at 18 you have, for example, a passport? Whereas some services allow users under the age of 13, Twitter does not, so how you verify the age of a nine year-old who might not have government ID is much more challenging.

Baroness Bertin: Let us face it, children under the age of 13 are on Twitter and they are taking part in conversations and forums that they are perhaps not mentally able to deal with, and that is where the big problems come with mental health and young children and all the rest of it. It cannot just be dismissed.

Nick Pickles: That is absolutely correct. We are engaging with DCMS on the Green Paper and a wide range of initiatives. Age verification has become seen as the silver bullet to solving a whole range of problems.

Baroness Bertin: You have said that quite a few times and I would pick you up on it. Of course, questions as to who is liable and age verification will not absolutely solve everything but even if they reduce some of these problems by 20%, we are in a better place than we were. I just want to make that point.

Nick Pickles: We all have an opportunity here to work through the consequences of those decisions because the unintended consequences, whether it be restriction in competition or free expression or the diversity of the services that exist, makes this a balancing act, and the work you are doing to understand these challenges is really important.

Q125 **Baroness Bertin:** Moving on to my question about competition law, obviously, both of your companies buy up rivals and have lots of different names under your brand. Do you think that it is right you are able to do that or do you think there is an issue there with competition law?

Jared Sine: I am happy to address that first. From our perspective, one of the things that we find, based on research, that most users multihome, which means they are using three or more dating apps in connection with their dating activities. Without the ability to offer a variety of different experiences that appeal to different demographics, different tastes and preferences, it becomes very difficult to ensure that you are offering a robust product set. From our perspective, we do not believe that acquiring businesses to provide our user bases with new and interesting services, or services that appeal to their different appetites or tastes and preferences, is something that should be restricted, to the extent that it is not violating the existing competition laws that are out there. We definitely look at those very closely in connection with any acquisitions that we do. I do not believe there should be some blanket prohibition on businesses acquiring other businesses in the same space, given, particularly in our space, the way that the user behaves and operates in the space.

Nick Pickles: We own a company called Periscope and that is quite different from Twitter. We do not own another company that has similarities to Twitter. To add to that, the one thing I would say is there is an interesting tension around industry working together to try to solve some of these problems. The Internet Watch Foundation works on counterterrorism through GIFCT and there is a question mark there around how competition regulators see companies working together to solve these kinds of challenges and decide whether that is anticompetitive behaviour. In counterterrorism work, we are working with smaller companies to help them learn from our experience, but not every small company has the same engagement because they might be less willing to talk to us. That is a question for competition regulators because we want to protect that kind of industry collaboration. The flip side in some of these competition issues is that industry is stronger challenging these by problems working together, and we want to maintain that.

Q126 **Lord Gordon of Strathblane:** You will have heard the Information Commissioner refer to the powers that her department now has to produce a code of practice about age-appropriate design. What principles do you think should be set out to govern that?

Nick Pickles: As the Information Commissioner rightly said, the UK is ahead of the game on this. Industry is increasingly thinking about it. Our CEO Jack Dawsey said last week that incentives are very important. When you are creating a service, what incentives are you putting there and how do people engage with it? There is a real opportunity for the UK to lead on this. Things such as transparency are important. We heard about making sure people know what they are signing up for. Twitter was rightly held to account for the fact that people felt we were not telling them why we were suspending their accounts. They just got a note saying, "You've been suspended". We now tell you the exact tweet that you have been suspended for and which rule it broke. Transparency builds trust and there should be transparency in both how you are using data and in allowing users to check in real time what you are doing with their data. We now allow people to click through in real time and see, "Which advertising categories have you put me in based on using my data?" Transparency is a key one for me.

Lord Gordon of Strathblane: Does Mr Sine agree?

Jared Sine: In terms of age appropriateness and full disclosure, we had the opportunity to sit down with Baroness Kidron and discuss some of this with her. We think it is a fantastic idea to have more age-appropriate approaches and regulatory regimes, again to the extent that they are tailored appropriately to ensure that, if you are targeting children or those under the age of majority, you are approaching it in a proper way. I agree with Mr Pickles that transparency in that respect is very important and, from our perspective, it is something we laud and we would generally support.

Q127 **Lord Allen of Kensington:** I think all my points have been covered. My question was on data protection and I was going to ask how you can ensure that people's data is processed fairly and transparently. I would like to come back to you, Mr Sine. You talked about the fact that you do not provide data to third-party organisations. Do you provide it in an anonymised way if it is not personally given? Secondly, you said that limited data was used for advertising. Can you explain that in a little more detail for me?

Jared Sine: In terms of our data that we use on our platforms, we do not provide data to third parties. In rare instances, we may have a partnership or relationship where we need to use anonymised data. For instance, we recently launched a location feature, and we have a partner who is helping provide location-specific data when someone is at a certain location to show what location they are actually at, so we have to provide some anonymised data to make sure that we get the right information back from that provider, but it is never user-specific information. Again, we share data with third-party providers who are providing services to help us conduct our services, but in general we do not have any need to share anonymised data with third-party organisations for commercial or other purposes that are not related to our services.

In terms of the targeted advertising, like many platforms, we have information as it relates to our users in terms of age categorisation, gender, et cetera, and if a brand comes to us and says, "We want to target this type or category of individual", we have data that allows us to make sure those advertisements are going to and addressing the appropriate audience, but we do not share that data back with the third party regarding the individuals who saw the ad, et cetera. We may give numbers because they have to understand the impressions and those kinds of things, but we do not provide the user-specific data back to those advertisers. Again, that is a very, very small part of our business.

Lord Allen of Kensington: I think you said 5%. Thank you. Mr Pickles.

Nick Pickles: Several points have already been covered. The interesting question here is that every business nowadays is a data business. It is not just internet companies; personal data is at the heart of pretty much every company now. The first thing about Twitter is we are a public platform which is quite different because people are tweeting publicly to the world their tweets and the overwhelming majority of tweets that are sent are sent publicly. That changes somewhat the nature of the conversation because it is being publicly expressed. For us, a global privacy policy is very important. We do not want a fragmented approach. We want all our users to understand that we have a very clear approach. I am happy to share a copy of our privacy policy because we have done a lot of work focusing on how to make it understandable, how to make it very clear what we are doing, how to make it clear what people can choose to control themselves and how that data happens, and how they can download their own data. Picking up on what the Information Commissioner said earlier, we are also working with peer companies to allow people to take their data to other companies. Data protection is about protecting data, but it is also about empowering users to control their information, and we think if you can move your data to another company and another service that makes for a more competitive open internet.

Lord Allen of Kensington: *Which?* did a survey recently and it gave us data that showed that 50% of people interviewed did not understand how their data was used. If I asked you how many Twitter customers understood your Ts and Cs and how their data would be used, what percentage would you put on that?

Nick Pickles: That is exactly why we separated our privacy policy from our Ts and Cs, because we wanted it to be a very clear stand-alone document. I used to run a privacy campaign group. I care very deeply about privacy. It is very heartening to see the public debate and conversation that is happening about privacy now. Whether it is about government use of data, corporate use of data, personal control, personal transparency, it is a phenomenonally good thing, and I think it will lead to a more informed public policy debate and savvier consumers. At the heart of all this are businesses, and savvy consumers are the best way of keeping businesses honest.

The Chairman: Can I thank both of our witnesses for the evidence they have given us? Mr Sine, do you have any closing comments or thoughts or anything that you think we might have asked and did not?

Jared Sine: No, I think we have covered the seafront from my perspective. Again, I want to state that from a Match Group perspective we are supportive of regulation in this area, again to the extent that it is carefully crafted, thoughtfully considered, and to the extent that industry is involved. We look forward hopefully to opportunities to continue to work with policy-makers and legislators to ensure that new regulation, to the extent it is developed, is consistent with those principles that we think are important.

The Chairman: Thank you. Mr Pickles.

Nick Pickles: First, may I thank you all for your thoughtful questions? There is a lot of heat on this issue right now and a lot of desire for quick solutions. The big challenge for us all is to think through how to protect free expression and the digital economy and to ensure that consumers are protected. Those three things stand together. I would be delighted to further assist the committee in its work as the inquiry continues.

The Chairman: Thank you again to both our witnesses for their evidence and thank you to those on either side of the Atlantic who made the technology work. We will be producing our report towards the end of the year and your input has been invaluable.

The Mayor of London – written evidence (IRN0094)

Introduction

1. The Mayor of London is grateful for the opportunity to submit to the Communications Committee Inquiry into Internet Regulation.

2. London is home to 9 million citizens and is a global hub for technology. While technology is creating whole new industries, revolutionising existing ones, and changing the way that transactions are made and content is consumed, it also has the potential to transform the experience that Londoners have of our city. London's tech community is spurring much of the innovation across Europe and the globe. The Mayor wants all Londoners, as well as businesses across different industries, to benefit from the opportunities presented by digital technology.

3. Our tech sector leads in the use of data and design, personalising services for citizens enhancing the enjoyment of content, networks and new ways to communicate. Given the ubiquity of technology in citizens' lives great cities like London have a role to play in promoting responsible tech: that innovation should not knowingly deepen existing vulnerabilities or cause new harms. Digital services, whether created or provided by the public or private sector, should be responsive to this as well as diversity and inclusion - and operate responsibly.

4. Social media companies must wield the power they've amassed responsibly. At South by South West, in March 2018, the Mayor shared his concerns about responsibility and social media platforms: *"Platforms, such as Facebook, Twitter, and YouTube have brought huge benefits to society. They've made it easier for us to stay in touch with those we love, meet like-minded people, and have easier access to information we want. They've enabled talented people to share their creativity directly with the world. But, understandably, there are* ***growing concerns about some of the ways the biggest companies on the planet have impacted our lives*** *and the overall wellbeing of our societies. In some cases, these new platforms have been used to exacerbate, fuel, and deepen the divisions within our communities. The impact is and continues to be profound and should worry democracies around the world."*

5. The Mayor has called on social media platforms to show a stronger duty of care, so that they can live up to their promise to be places that connect and unify, not divide and polarise.

6. In collaboration with his Office for Policing and Crime (MOPAC), the Mayor has established an Online Hate Crime Hub. The Hub is comprised of five dedicated Met police officers working in partnership with community groups, social media organisations, academic hate crime specialists and criminal justice partners to improve the police response to online hate including abuse on Twitter and Facebook.

7. The Hub was developed out of concern from community organisations around the increasing use of social media and the internet to spread hatred against

minority and vulnerable groups and individuals. It is the first of its kind in the UK and is helping to tackle online hate crime and improve support for victims across the capital, as part of the Mayor's manifesto commitment to a zero-tolerance approach to hate crime.

8. The Mayor has also brought together national and international experts in tackling online hate and extremism at an Online Hate Crime Summit. Representatives from Twitter, Facebook, Crown Prosecution Service, the Met and charities joined victims of online hate at City Hall to discuss how they can work better together to tackle online hate and support those affected by it.

9. The onus for change is not just on tech companies and innovators. It must ultimately fall to government, working in partnership with these companies and leaders to ensure that the technology revolution is not detrimental to our long-term progress.

Is there a need to introduce specific regulation for the internet? Is it desirable or possible? What should the legal liability of online platforms be for the content that they host?

10. Rather than a specific regulation for the internet, we should consider the means to encourage/enforce responsible behaviour from individual companies.

11. It's extremely positive that social media platforms have revolutionised the way communities are able to communicate and share information with each other, and created opportunities for users to promote their own creative content without having to go through something like a publisher, an agent or a record company.

12. However, maintaining those benefits must be balanced with the need to control the promotion of hate, extremism and violence which are incredibly widespread. Victims of hate crime often suffer lasting trauma and take longer to recover than victims of other forms of harm. Online victims are especially isolated, vulnerable and invisible. It is incumbent both on social platforms and government to develop the right mechanism to police online behaviour.

13. Recent legislation banning illegal hate speech online in Germany provides an interesting case study. Facebook and Twitter have worked with the German authorities, employing additional moderator staff and adding additional features to their platforms, to make sure that this rule is enforced. Companies are now operating much more quickly and effectively.

14. The Mayor recognises that some social media companies seem to have responded promptly and effectively but there is a discussion to be had about whether this is precisely the right approach, striking the right balance between freedom of speech and freedom from abuse. Either way, it shows that it is possible for companies to work in different ways in different countries in order to comply with local rules.

15. The Mayor is particularly concerned over the length of time it takes for harmful content to be removed. Harmful content can go viral in minutes; removal targets

should be a matter of hours rather than days, weeks and months, if we are going to limit the spread of harmful material.

16. Social media platforms already have a legal obligation to remove content that breaks laws, such as those around hate speech. But this is not always happening or happening quickly enough. Facebook, Twitter and other platforms are starting to react to the criticisms and are developing technology to make sure the reporting process becomes quicker and more effective. This is positive but does not go far enough.

17. Users should only be relied upon to flag certain types of content such as videos or messages seeking to incite violence as a backstop option. Social media companies should seek to develop mechanisms to identify for example knives and other weapons and delete them before they are uploaded. If companies can develop algorithms which can target users with offers and adverts based on their online interactions, likes and searches across different platforms, that skill and expertise should also be able to create algorithms which can be deployed and used to address issues of hate.

What role should users play in establishing and maintaining online community standards for content and behaviour?

18. 'Civil society' initiatives, such as the 'Re-Claim the Internet' campaign, aimed at encouraging and supporting 'active citizens' to use platform based reporting mechanisms in response content perceived to be offensive or indecent, are positive and should be supported.

19. Whilst private citizens play a critical role in establishing a culture of inclusion and tolerance online, and in challenging harmful behaviour, they cannot be expected to hold sole responsibility for policing each other.

How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

20. We need to get the balance right between open platforms which create the freedom for people to place their creative content in front of an audience and making sure we control the online promotion of hate, extremism and violence which unfortunately we are seeing increasing in volume. Ultimately it is incumbent both on social platforms and government to make sure the way we police social media is up to the job of doing that.

21. While a small number of major providers may have improved their approaches of using reporting, evidence from the Stop Hate UK Helpline services is that moderation process is neither transparent nor effective. Delays between reporting concerns and any action taken are often significant. Decisions are often poorly explained if at all. There also appears to be a lack of consistency and clarity over how decisions regarding the removal of content, once reported, are made. This inconsistency and lack of clarity is likely to discourage users from using the available reporting mechanisms.

What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

22. We have to be very careful to get the balance between freedom of speech and freedom from abuse right. People must have their legitimate right to say things that others don't like protected. But this must go hand-in-hand with the right not to be abused or intimidated. The Mayor is intending to monitor the impact of the German legislation referred to above carefully, in order to assess its impact on freedom of expression.

May 2018

Metropolitan Police, Internet Watch Foundation, National Crime Agency and National Police Chief’s Council – oral evidence (QQ 35-43)

Transcript to be found under Internet Watch Foundation

Microsoft UK – written evidence (IRN0085)

Microsoft in the UK

Microsoft seeks to empower every person and organisation on the planet to achieve more. We provide products and services relating to nearly every facet of the digital ecosystem, including software, hardware and cloud services. Our UK workforce totals around 5,000 people across 5 offices. The UK is also home to our European research lab, Microsoft Research, which employs over 120 of the world's leading computer scientists in Cambridge. We have a 25,000 strong UK partner network, employing over 800,000 people and generating over £38 billion pounds in attributable revenue.

Microsoft is committed to developing the UK's digital skills and our Microsoft Partner Apprenticeship programme has created more than 15,000 apprenticeships in the six years since its creation. It is now responsible for nearly a third of all IT apprenticeship starts and we are committed to seeing a further 30,000 starts by 2020.

Microsoft's services offered in the UK are broad and include the following:

- Productivity tools within the Office and Office 365 suite, such as Word, Outlook and PowerPoint
- The full range of Cloud services, Azure, which includes various AI and data analytics capabilities
- Microsoft Consulting Services
- The search engine Bing
- Xbox, including the platform and games
- Devices, including the Surface range of notebooks and tablets
- LinkedIn, which is owned by Microsoft

Executive Summary

- Microsoft supports continued debate on how best to regulate the online world. Indeed, as technology progresses, and society takes time to develop the familiarity with these new services, regulation can play an invaluable role in building confidence and trust in technology. Microsoft welcomes the opportunity to be part of this discussion and the opportunity to submit evidence to the House of Lords Communications Committee's inquiry on internet regulation.

- The internet is supported by a delicate and complex ecosystem of interweaving UK and EU legislation. This includes laws governing connectivity, intellectual property, copyright, net neutrality, data protection and privacy, to name a few. It is in fact only made possible by regulation. This shift in perception has an important implication – by understanding that the internet is underpinned by various laws, emphasis shifts from a purely regulatory focus and recognises that the challenges posed by the internet typically require enforcement of existing laws and regulations, and not new legislative or regulatory responses. Contrary to the commonly heard dictum, *what is illegal offline is almost always illegal online*.

- Limitations to liability for online intermediaries, set out in Articles 12-15 of the eCommerce Directive, play a foundational role in the regulation of the internet. Crucially, intermediary liability focuses on the *activities* of organisations, rather than business models or types of companies. This makes these regulations adaptable to a range of different digital environments as can be seen by the wide range of Microsoft services set out above that are subject to these rules. As such, these regulations are technology neutral and apply in a highly targeted manner. This is important because many companies have highly complex business models, meaning they may be an intermediary for some activities but not for others.

- Microsoft supports the goal of reducing the amount of illegal content online and we recognise that technology platforms have important responsibilities in achieving this shared goal. We encourage the Committee to recognise there is no "one size fits all" approach given the multifarious applications of the current intermediary liability regime. Rather, the Committee must take account of the critical fact that different types of services and different types of content merit different consideration.

- The EU has played an important role in harmonising regulation that enables digital growth across Members States. These are various, ranging from net neutrality to data protection, and have provided legal clarity and regulatory certainty for companies operating in the EU. Many of these rules underpin the cross-border nature of the digital economy so it is critical that any regulatory divergence post-Brexit does not result in the establishment of non-tariff barriers for digital trade. Given the ongoing digitisation of the wider economy, this is just as important for non-tech companies as for tech companies.

Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

1. Microsoft supports continued debate on how best to regulate the online world. Indeed, as technology progresses, and society takes time to develop the familiarity with these new services, regulation can play an invaluable role in building confidence and trust in technology. Microsoft welcomes the opportunity to be part of this discussion and the opportunity to submit evidence to the House of Lords Communications Committee's inquiry on internet regulation.

2. The UK consistently ranks among the world's leading digital economies on a range of metrics including: foreign direct investment (FDI), venture capital investment, digital maturity, GVA and research base. As such, it is one of the jewels in Britain's industrial crown.[958]

What is illegal offline is typically illegal online – towards an enforcement approach

[958] See e.g. Tech City UK (2017) Tech Nation; European Commission (2017) Digital Society and Economy Index (DESI); Tufts University (2017) Digital Evolution Index.

3. The internet is supported by a delicate and complex ecosystem of interweaving UK and EU legislation. This includes laws governing connectivity, intellectual property, copyright, net neutrality, data protection and privacy, to name a few. Microsoft recognises that the rapid transformation facilitated by the internet poses new policy questions, many of which require innovative responses, but it is important not to perceive the internet as an unregulated domain. It is in fact only made possible by regulation. This shift in perception has an important implication – by understanding that the internet is underpinned by various laws, emphasis shifts from a purely regulatory focus and recognises that the challenges posed by the internet typically require enforcement of existing laws and regulations, and not new legislative or regulatory responses. Contrary to the commonly heard dictum, *what is illegal offline is almost always illegal online*.

4. The belief that the legality of certain actions is different on the internet contributes towards an unhelpful framing of the very real policy questions that need to be addressed in this area. The debate between rights holders and technology firms over copyright infringement is a good example: the issue is not whether new laws need to be made to criminalise copyright violations online, these are already illegal. Rather it is about enforcing these laws in the online world. In this case, a successful notice and takedown system has emerged in the UK, supported by a new voluntary code between rightsholders and technology firms. This set out mutually agreed targets for the removal of search engine links to copyright infringing sites. Monitoring is overseen by the Intellectual Property Office and the March 2018 search measurement showed that both Bing and Google pass the compliance goals set out in the code.

5. Recognition that many of these questions are typically ones of enforcement also underlines the need for multi-stakeholder responses. The issue of child sexual abuse material (CSAM) is a case in point. Technology companies have developed effective technical tools to identify infringing material – Microsoft’s PhotoDNA technology was a pioneering technology in the ongoing fight against this most heinous of issues. As a responsible technology company, Microsoft responds to law enforcement requests for the removal of potentially infringing images, through a well-defined and legal process, helping to ensure this material is not hosted on our servers, while protecting the privacy of our users. This long-established relationship has been critical in the ongoing fight against CSAM. Regulation in one area often impacts the ability to act in another and worryingly, we have concerns about the unintended consequences of the ePrivacy Directive currently making its way through European legislative procedures, restricting our ability to proactively scan content that would help in the fight against CSAM.

6. This reframing also underlines the fact that generic questions often yield overly broad answers to the challenging policy issues posed by the internet. Rather than a generic question about regulating the internet, focus should instead be on asking specific questions emerging from clearly identified policy challenges. Given the wide range of economic and social activity underpinned by the internet, Government should consistently measure the broader impact of any proposals for internet regulation as a one-size-fits-all approach is unlikely to be appropriate.

What should the legal liability of online platforms be for the content that they host?

Intermediary Liability

7. As mentioned, the internet is far from an unregulated space - it is underpinned by a framework of laws and norms that delicately balance the rights and responsibilities of the wide range of organisations in the digital ecosystem. The digital ecosystem consists of a wide variety of companies including ISPs, providers of cloud services, search engines, advertising platforms, social media companies, rightsholders and others.-The cornerstone of this framework is certain limitations to liability for online intermediaries, set out in Articles 12-15 of the eCommerce Directive.[959]

8. Articles 12-15 set out the specific conditions under which providers of "information society services"[960] are immune to liability for illegal content being transmitted in the provision of a service (and conversely the conditions under which they are liable). These activities can include the sale of goods, the transmission of information via communications networks, the comments section on a newspaper website, or hosting information provided by a recipient of the service (e.g. cloud hosting services or website hosting). In Microsoft's case, these services could include OneDrive, Bing, LinkedIn, and our gaming platform, Xbox Live.

9. Crucially, intermediary liability focuses on the *activities* of organisations, rather than business models or types of companies. This makes these regulations adaptable to a range of different digital environments as can be seen by the wide range of Microsoft services set out above that are subject to these rules. As such, these regulations are technology neutral and apply in a highly targeted manner. This is important because many companies have highly complex business models, meaning they may be an intermediary for some activities but not for others – for example, a newspaper site is a publisher of its news content but its user comments sections are under the scope of intermediary liability. Intermediary liability then, as set out in the eCommerce Directive, provides critical legal certainty and clarity for companies across the various activities they undertake.

Differences in platforms and content require individual consideration

10. Microsoft supports the goal of reducing the amount of illegal content online and we recognise that technology platforms have important responsibilities in achieving this shared goal. We encourage the Committee to recognise there is no "one size fits all" approach given the multifarious applications of the current intermediary liability regime. Rather, the Committee must take account of the critical fact that different types of services and different types of content merit different consideration.

11. We urge the Committee to differentiate between the types activities that take place on individual platforms. Services such as social media and video sharing

[959] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

[960] An "information society service" is defined as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services" in Article 1(2) of Directive 98/34/EC.

platforms, which are often specifically designed to enable broad sharing of content, are used differently by consumers than cloud storage services, private messaging platforms, topic-specific platforms (such as gaming platforms) or professional networking platforms. As such, they raise qualitatively different risks than these latter services, which are intended primarily for private communications.

12. Service providers should be given the ability to tailor responses in light of the unique risks and harms posed by different categories of illegal content. For example, using automated technologies (with appropriate safeguards in place) might be appropriate with regard to illegal content such as CSAM, but less suitable for other types of content where determining illegality may be more complex or subjective (e.g. hate speech). The current intermediary liability regime provides the flexibility for companies to be able to do this.

13. Calls for reforms to intermediary liability are often motivated by a small number of highly challenging issues such as hate speech, online extremism and intellectual property found on a limited number of platforms. As such, policymakers must take care not to take a sledgehammer to a nut when considering how to respond to these pressing issues.

The need for an economic impact assessment

14. The Department for Digital, Culture, Media and Sport (DCMS) will consider the liability regimes governing platforms as part of the *Digital Charter*.[961] Given the foundational role intermediary liability plays in the digital ecosystem, we would urge the Committee to call on the Government to undertake an extensive impact assessment examining any proposed changes to this regime. A June 2017 analysis by the Internet Association found that weakened intermediary liability could cost the US economy 4.25 million jobs and close to half a trillion dollars in lost economic activity over the next decade, highlighting the critical role intermediary liability plays in driving economic growth and digital innovation.[962] This is a staggering figure and provides a compelling reason for similar research to be carried out by the Government. We understand that no such research exists in the UK.

How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

In what ways should online platforms be more transparent about their business practices – for example their use of algorithms?

What information should online platforms provide to users about the use of their personal data?

Moderation varies by platform and content, as do penalties

[961] Department for Digital, Culture, Media and Sport, *Digital Charter* (see "Work Programme").
[962] Internet Association (2017) Economic Value of Internet Intermediaries and the Role of Liability Protections

15. Content moderation comes in various forms, relative to the platform or service in question. It is not a homogenous activity. For example, at Microsoft, we might variously moderate user content on our Xbox Live network to ensure the safety and security of our users or Bing search results to bring greater relevance for our users. We also have systems in place to prevent sharing of illegal content, such as CSAM, on our services, like OneDrive. Microsoft believes transparency is vital and we publish a biannual transparency report that covers a wide range of activities including law enforcement requests for user data and content removal requests, among others.[963]

16. Microsoft typically moderates illegal content so the consequences for those accounts implicated in sharing this material are usually severe. Our Microsoft Services Agreement, which covers all our products and includes a Code of Conduct, explicitly prohibits illegal activity, as well as a wide range of harmful activities such as abuse, sharing inappropriate content, or false or misleading activity.[964] Violating these terms can result in a range of sanctions, depending on the service and the infringement, and ultimately we may close a user's account. Where accounts are closed, we typically do not permit them to be reopened where they have engaged in illegal activity. In so far as search results can be thought of as "moderated", we make our guidelines clear in our Bing Webmaster Guidelines.[965]

17. Other platforms may moderate content in a different manner. For example, social media platforms or video sharing sites may moderate content in a way that is more akin to content "curation", in that they tailor information believed to be of maximum interest to their users. With the exception of LinkedIn, Microsoft does not provide products or services that would curate content in such a manner. The LinkedIn news feed typically provides users with posts from business connections, or individuals and organisations users choose to follow.

Algorithmic accountability is a more helpful approach than transparency

18. Microsoft believes that there should be accountability around the use of algorithms. While we understand the increased focus around transparency as a means to achieve accountability, we believe more thinking needs to be done to identify the best approach.

19. Because of complexity of algorithms, algorithmic "transparency" does not necessarily enable "accountability." AI tools are driven by a complex combination of algorithms. Putting this type of complicated code into the public domain for everyone to inspect will likely do little to drive accountability. By way of example, a vulnerability known as the 'Heartbleed' vulnerability was introduced into a piece of open source code in 2011. Being open source, this piece of code was publicly available and widely used with thousands of web servers relying on it for security. Thousands of specialist computer scientists worked on the code on a regular basis and yet the vulnerability was not identified until 2014. In this instance, there was

[963] Our Transparency Reports can be found on Microsoft's Transparency Hub

[964] Microsoft Services Agreement

[965] Bing Webmaster Guidelines

total transparency regarding a publicly available algorithmic code, and yet it still took two-plus years to identify an algorithmic vulnerability.

20. Moreover, knowing the workings of a piece of algorithmic code is of little use in understanding its functions unless the algorithm's inputs, e.g. data source, are also observable. Take for example a social media newsfeed. Such systems are designed to adapt based on user feedback such as clicks and interactions, resulting in a 'personalised' newsfeed. 'Personalisation' is based not just on your data but a weighting of your data against the data of other users. Accordingly, such a newsfeed is compiled by comparing the data that's input into the system – via interactions – with the data of other users, so that the search results that surface are statistically relevant to the results that appear for others. Detailed information about the media algorithm alone would be of little value in understanding why the algorithm delivered the outputs it did, and gaining access to the full set of data inputs would present significant questions about user privacy.

21. A more detailed consideration of this topic is available in Microsoft's submission to the House of Commons Science & Technology Committee inquiry into algorithmic transparency.[966]

Companies must be allowed to protect their intellectual property

22. Algorithms are also intellectual property and companies must be entitled to fully protect their trade secrets and confidential business information, as in any other sector. Desire for transparency must be tempered with the right to confidentiality of sensitive business information so as not to divulge any intellectual property.

23. We urge the Committee to also recognise the ubiquity of algorithms across all businesses and sectors – they are not only employed by technology companies. This recognition is important to ensure technology companies in the UK are not placed at a competitive disadvantage through well-intentioned but disproportionate transparency requirements. This is especially true where transparency does not necessarily lead to greater accountability, as can be the case with algorithms.

AI and transparency

24. Transparency and accountability are crucial concepts to ensuring the fair use of AI. Microsoft is playing a leading role in developing an ethical framework for the use of AI. In our recent book, *The Future Computed*, we set out six values AI systems must respect: fairness; reliability & safety; privacy & security; inclusiveness; transparency; and accountability, where transparency and accountability are understood as foundational principles.[967]

[966] Microsoft written evidence to House of Commons Science & Technology Committee inquiry on fairness and transparency in algorithmic decision making: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/algorithms-in-decisionmaking/written/69163.html

[967] Microsoft (2018) *The Future Computed* esp. pp.52-84.

25. When AI algorithms are used in making decisions that impact people’s lives, it is particularly important that people understand how those decisions were made. An approach that is most likely to engender trust with users and those affected by these systems is to provide explanations that include contextual information about how an AI system works and interacts with data. Such information will make it easier to identify and raise awareness of potential bias, errors and unintended outcomes.

26. Simply publishing the algorithms underlying AI systems will rarely provide meaningful transparency. With the latest (and often most promising) AI techniques, such as deep neural networks, there typically isn’t any algorithmic output that would help people understand the subtle patterns that systems find. This is why we need a more holistic approach in which AI system designers describe the key elements of the system as completely and clearly as possible.

27. Microsoft is working with the Partnership on AI and other organisations to develop best practices for enabling meaningful transparency of AI systems. This includes the practices described above and a variety of other methods, such as an approach to determine if it’s possible to use an algorithm or model that is easier to understand in place of one that is more complex and difficult to explain. This is an area that will require further research to understand how machine learning models work and to develop new techniques that provide more meaningful transparency.

Microsoft gives users transparency and control over their personal data

28. Microsoft strives to remain transparent in its business practices. For example, the Microsoft Privacy Statement sets out in detail the personal data we collect, how we use personal data and how individuals can access and control their personal data. The Microsoft Privacy Dashboard allows users to see and control activity across multiple Microsoft services including browsing, search, and location data associated with their Microsoft account. We also provide users with product-specific privacy details, for example around Windows, enterprise and developer products, and search and artificial intelligence (AI).

What measures should online platforms adopt to ensure online safety and protect the right of freedom of expression and freedom of information?

What role should users play in establishing and maintaining community standards for content and behaviour?

Balancing security and fundamental rights

29. Microsoft works hard to balance the safety and security of our users and customers with fundamental rights to privacy, freedom of expression and the right to access information. Although Microsoft does not run any of the leading social networks or video-sharing sites, from time to time, illegal or harmful content may be posted to or shared on our Microsoft-hosted consumer services. Tackling this content is be done in a number of ways, depending on the nature of the content and the service. There may be technical tools to flag potential or

known illegal, as in the case of CSAM, or we may go through well-established "notice and takedown" procedures, for copyright violations.

30. The technology industry is actively working towards developing effective solutions for the early detection and removal of illegal content and has already made significant headway, in particular with respect to the sharing of previously identified illegal content. Solutions include PhotoDNA (mentioned above) and the cross-industry hash-sharing database for egregious terrorist content via the Global Internet Forum to Counter Terrorism. Each of these initiatives was set up and is managed voluntarily by industry, all of whose participants share the goal of removing these types of illegal content from the Internet. Microsoft is proud to participate in these initiatives.

Legal and ethical considerations around the use of automated tools

31. As we develop these solutions, we are acutely aware that the use of automated technologies poses risks to these fundamental rights. Automated tools may, in certain circumstances, result in service providers removing lawful content, especially where the lawfulness of the content is context-specific or where the legality of the content varies between countries. It is important to note that changes to intermediary liability could result in service providers erring on the side of over-removal of content in order to minimise liability risks. As such, any blunt regulation that would require companies to use automated tools – even with safeguards such as human oversight in place – could result in the removal of lawful content, undermining users' rights to receive and impart information.

32. There are also broader ethical and technical considerations raised by the use of automated tools to identify and remove content which go beyond encroachment of users' fundamental rights. Echoing the previous section on AI and transparency, difficult questions arise as to whether commercial entities' transparency regarding algorithmic-based decision-making, especially when powerful, automated tools are used to determine and monitor what and how much information we, as a society, are permitted to see online. For example, AI-driven algorithms may disproportionately remove minority views or (inadvertently) target content that reflects minority positions. Alternatively, bad actors may use these tools to maliciously influence content available online. Companies, including Microsoft, are only beginning to explore issues around bias and ethics in this regard. The technology is not yet able in many cases to accurately detect content without numerous false positives or negatives – forcing its use before it is reliable, could lead to unwanted infringements on individual liberties.

33. Policymakers must be alert to these tensions when considering any new obligations on companies to proactively remove content. There must be clear guidance on how they may do so consistent with their obligations under the GDPR or other relevant UK law (and EU law, until the UK formally leaves the Union). This would include the impact on any future data flows agreements between the UK and EU.

Defending democracy in a digital age

34. In light of recent concerns about fake news and the integrity of democratic processes, Microsoft recently launched its Defending Democracy Programme. In our January 2018 *Top Ten Tech Issues For 2018* report, we identified this year as a critical one for governments and technology companies to work together to safeguard electoral procedures.[968] Heeding our own call to action, Microsoft's Defending Democracy Program will work with stakeholders in all democratic countries to defend against disinformation campaigns; increase political advertising transparency online; protect campaigns from hacking; and explore technological solutions.[969]

35. As technology changes the way we consume information and our political engagement, Microsoft believes tech companies have a special responsibility to ensure the resilience of our democratic systems.

Xbox users are key to ensuring user safety on Xbox Live

36. Microsoft also believes the users a key role to play in fostering a safe and happy community. Our Xbox Ambassadors are a network of passionate and knowledgeable Xbox fans who strengthen the Xbox community by supporting fellow gamers.[970] This includes chat support, hosting Mixer shows and creating a library of content to help other gamers. We have also launched Gaming for Everyone, an initiative that aims to promote diversity and inclusion in the Xbox community.[971] This both promotes diversity among gamers but also diversity by design.

37. This is in addition to a wide range of Xbox Live safety features, underpinned by its own Code of Conduct.[972] As well as illegal content, this includes a prohibition on content that could harm or harass a person such as (but not limited to) profane words or phrases; negative speech directed at people who belong to a group, including groups based on race, ethnicity, nationality, language, gender, age, disability, veteran status, religion or sexual orientation/expression; "noise", which is excessive speech intended to interfere with or disrupt another person's or group's ability to enjoy a game or app on Xbox Live.

What effect will the UK leaving the EU have on the regulation of the internet?

Continued data flows with the EU must be a priority

38. The EU has played an important role in harmonising regulation that enables digital growth across Members States. These are various, ranging from net neutrality to data protection, and have provided legal clarity and regulatory certainty for companies operating in the EU. Many of these rules underpin the cross-border nature of the digital economy so it is critical that any regulatory divergence post-Brexit does not result in the establishment of non-tariff barriers for digital trade.

[968] Microsoft (2018) *Today in Technology: The Top 10 Tech Issues for 2018*
[969] More information on Microsoft's Defending Democracy programme can be found here: https://blogs.microsoft.com/on-the-issues/2018/04/13/announcing-the-defending-democracy-program
[970] More information on Xbox Ambassadors can be found at https://community.xbox.com/ambassadors.
[971] More information on Gaming for Everyone is available here: https://news.microsoft.com/gamingforeveryone/
[972] Xbox Live Code of Conduct

Given the ongoing digitisation of the wider economy, this is just as important for non-tech companies as for tech companies.

39. The continuation of cross-border flows of personal-data is particularly important for the UK economy and Microsoft supports the Government's vision for an "adequacy+" decision, as set out in the Prime Minister's Mansion House speech and by the Secretary of State for Digital, Culture, Media and Sport.[973] We particularly welcome the Government's decision to implement GDPR in full, as regulatory equivalence with EU data protection standards is absolutely necessary to securing an adequacy decision (or similar) with the EU that will permit continued data flows.

The UK should pioneer a new approach for including digital trade in Free Trade Agreements

40. Digital trade is an area in which Brexit provides the UK Government with post-Brexit opportunities. No Free Trade Agreement (FTA) has yet provided a comprehensive deal for the free flow of data. We would encourage the UK Government to be ambitious in any new trade deals it negotiates by developing a "digital chapter" that writes data flows agreements into future FTAs. This should seek to allow maximum data flows between parties, for example by removing data localisation requirements.

41. However, any developments in this area must not come at the expense of a data flows agreement with the EU. The continued flow of data between the UK and EU must be the first priority post-Brexit.

May 2018

[973] Prime Minister's speech on our future economic partners, hip with the European Union, 2 March 2018

Microsoft UK, Facebook UK and Google UK – oral evidence (QQ 174-182)

Transcript to be found under Facebook

Microsoft UK – supplementary written evidence (IRN0125)

Answers to additional questions raised by the Committee

How much tax do you pay in the UK as percentage of your turnover?

Our most recent audited financial statements show an annual UK turnover of £1,121,044,000 and tax per accounts as £29,141,000. This means tax as a percentage of turnover is 2.6%. We note that UK corporation tax is calculated as a proportion of profits rather than turnover.

Could the establishment of a new horizon-scanning body help to coordinate and empower regulators in the face of an ever-changing digital environment?

As the economy increasingly digitises, every sector is becoming a “tech” sector, so to speak. While a horizon-scanning body may have some value in coordinating and empowering regulators, it may be challenging for such a body to have the requisite sector-specific knowledge to provide a robust level of insight to specific regulators. The digital transformation of industries can have a sophisticated interplay with regulatory issues which a horizon-scanning body may struggle to grasp without sufficiently detailed knowledge of any given regulator’s beat.

A more robust approach may be in ensuring existing regulators have the requisite technical expertise themselves. The reasons are two-fold: firstly, sector-specific regulations should always be prior – these set the boundaries within which the application of technology can operate; secondly, it may be easier for each regulator to gain a sufficient level of technical knowledge than to expect a horizon-scanning body to have sufficient knowledge across all regulated sectors.

What lessons have you learnt from the processing of applications for the ‘right to be forgotten’? Could this model be used for the processing of complaints about other types of harm?

Microsoft’s search engine, Bing strives to promote the fundamental right of access to information while respecting local law in the markets where it operates. Bing’s experience processing applications for the Right to be Forgotten (RTBF) has reinforced the longstanding challenge facing search engines – striking the appropriate balance between individual privacy rights and the public right to access information.

Bing does not recommend expanding the RTBF model as it exists today. This is because it requires search engines to make substantive decisions about the law. Microsoft does not believe it is appropriate for a private company to be responsible for making substantive decisions about whether individual privacy rights trump the public right to access information, for example. We believe these sorts of legal decisions should be made by objective third parties rather than private companies.

Existing models that address these concerns are those where Bing receives a court order confirming content should be removed, or the U.S. Digital Millennium Copyright Act where intermediaries are required to block the offending content so long as a rightsholder completes the appropriate paperwork.
In each instance, Microsoft defers to an authoritative third party to make the substantive determination as to when content must to removed in order to protect individual rights.

Should the law around mergers and acquisitions be changed to create a public interest test (similar to that used in media pluralism cases) in cases of mergers between companies which rely on the use of personal data?

Microsoft is not a company that relies on the use of personal data. Microsoft predominantly sells enterprise software and cloud services to companies providing them with the ability to make use of their own data. As such, we do not have a view on a public interest test for companies that who's business models rely on the use of personal data.

Some have suggested that social media companies should be required to have their community standards approved by an external body, and for that external body to have the power to ensure that those standards are implemented? What assessment have you made of this proposal?

Microsoft is not a social media company, it is primarily a cloud services company. It does own LinkedIn, but this operates independently and has robust community standards[974].

The Microsoft Services Agreement sets out strict guidelines for all our consumer and enterprise services. This includes an explicit Code of Conduct[975] which is enforced across all our services. The Code of Conduct is significantly more restrictive than the law in terms of what is permitted on our services, especially when it comes to speech. This is because Microsoft believes certain behaviours are not acceptable on our services and our users should not have to encounter these experiences.

December 2018

[974] https://www.linkedin.com/help/linkedin/suggested/34593/linkedin-professional-community-policies?lang=en

[975] https://www.microsoft.com/en-us/servicesagreement

Motion Picture Association – written evidence (IRN0089)

The Motion Picture Association (MPA) welcomes the opportunity to respond to the Committee's inquiry into regulation of the internet. As a major part of the audio-visual sector in the UK the MPA represents companies that produce some of the highest quality and most popular creative content. Production of film and high end television is now a digital end-to-end process and our services and content are consumed increasingly through online platforms.

The MPA supports the definition of an online platform that was developed by the European Commission: *"online platforms cover a wide range of activities including online marketplaces, social media and creative content outlets, application distribution platforms, price comparison websites, platforms for the collaborative economy as well as online general search engines.*

They share key characteristics including the use of information and communication technologies to facilitate interactions (including commercial transactions) between users, collection and use of data about these interactions, and network effects which make the use of the platforms with most users most valuable to other users".[976]

However, many platforms falling within this definition operate illegally. In every category outlined above, it is possible to operate a business in full compliance with the law, but equally possible - and unfortunately very common among audio-visual platforms - to operate online businesses that disregard legal requirements for copyright, as well as in areas of consumer protection, taxation and data privacy.

Further government action needed

The MPA has welcomed the discussion of platform responsibility that is underway by UK and European policymakers and which, in some areas, is now well advanced with key legislative tools already in place at an EU level (for example mechanisms providing for no-fault injunctive relief against intermediaries to stop piracy). The key principle, we believe, is that online platforms must take ***proactive*** measures to detect/remove illegal content online – and not only react to notices received. They should also refrain from providing their services to anonymous operators.

There should be clearly defined responsibilities for platforms, including, but not limited to:

- Tackling the availability of illegal, harmful and infringing content on sites and services that they host - using a variety of proactive tools (filtering, artificial intelligence) and reactive measures (including notice and staydown).
- Ensuring sufficient transparency from registrants to support enforcement against illegal, harmful and infringing content.

- Providing rightsholders and law enforcement with sufficient information to identify and report illegal, harmful and infringing content.

[976] https://ec.europa.eu/digital-single-market/en/online-platforms-digital-single-market

Therefore in practice, platforms should be responsible for acting against illegal (including infringing) content available on, or promoted via, their platforms. They should take a swift, proactive approach to prevent the availability of - and take down - such content. They must also demonstrate a commitment to public education to ensure users are better able to identify infringing, illegal or harmful content and understand how to report it. In addition, platforms should do more to ensure that service providers using their platforms comply with Article 5 of the E-Commerce Directive on online transparency. In many cases this is currently being disregarded by those seeking to cause harm to other users (including members of the public) by spreading malware and by facilitating the proliferation of fraud and other "scam" activity, network infections as well as content that infringes copyright.

We recognise that there are a variety of avenues and policy levers that could be utilised to ensure platforms accept responsibility and take action against illegal, harmful and infringing content, including efforts that are being undertaken by ISPs, advertisers, and other intermediaries. Current approaches include, for example, "follow-the-money" strategies and voluntary site blocking arrangements. There are also several options for potential legislative change such as reform of the E-Commerce Directive to allow, for example, an SME threatened by the linking to and/or hosting of copyright infringing content to be able to bring a case against a platform that has not responded and acted to take down that content.

We believe that, in the first instance, the UK Government should use mechanisms such as the Digital Charter and the upcoming series of roundtables announced within the Creative Industries Sector Deal to ensure online platforms are doing all they can to ensure consumer safety online. Specific sets of roundtables are due to address social media and user upload platforms, as well the digital/online advertising industry and online retail marketplaces. The processes will seek to establish a voluntary code of practice for each area if one or more sufficient issues are identified and confirmed via the initial phase of discussions. The MPA believes that both platforms and rightsholders must be involved in all of these discussions in order to ensure that commitments are sufficiently wide-reaching and address illegal, harmful and infringing content (including advertising and problematic links). We welcome the Government's commitment to consider further regulation if effective voluntary codes of practice are not agreed by the end of 2018, and we look forward to working with the Intellectual Property Office and others to ensure that tangible progress is made.

About the Motion Picture Association

The MPA is the international trade association for the major companies that invest in, produce, distribute and market film and TV content in the UK, as well as being responsible for an increasingly wide variety of associated businesses and infrastructure initiatives. Our member companies include Disney, Fox, Paramount Pictures, Sony Pictures, Universal and Warner Bros.

The UK is one of the most important markets we operate in and MPA member companies are keen to work with the UK Government to maintain the UK's status as a world-leading hub for the film and television industries. Our companies are significant inward investors into the UK – and several of them have a strong permanent presence here including owning and operating major production facilities and running production companies in the UK.

The UK has become a world leading hub for film and TV production by creating a supportive environment through the combination of the highest quality technical skills, value fiscal incentives and a robust copyright framework. In particular, an effective copyright enforcement regime is a key element in creating an environment conducive to investment and growth. Content creators must be able to benefit from their creative endeavour in order to encourage significant and sustainable investment in new creative content. Protecting this investment in-turn ensures that UK consumers continue to be provided with a diverse range of the highest quality content across the AV industries.

Call for evidence

2. What should the legal liability of online platforms be for the content that they host?

The MPA believes that the responsibility to ensure illegal, harmful or copyright infringing content is not available on online platforms rests with the platform.

The MPA welcomed the recognition by the European Commission in September 2017 that an online information service (platform) is liable for copyright infringement if, when notified of infringement on its services, it does not act *"expeditiously to remove or to disable access"* to infringing content (Article 14 E-Commerce Directive). Similarly the Commission's view[977] is that online platforms must take proactive measures to detect and remove illegal content online, and not only react to notices received. This is a view supported by the MPA. As the Commission notes[978], a platform with a proactive approach to detecting and removing illegal content does not automatically lose its protection under the liability exemption. Online platforms remain exempt from liability when acting expeditiously.

Platforms must therefore undertake a range of proactive measures to address any illegal, harmful or infringing material or activity hosted on their digital "real estate". It is not sufficient for these measures to be simply reactive. There are a range of measures platforms can take, including; content filtering (to prevent the uploading of content or the offering of links in the first place), de-ranking, de-listing and promotion of legal content sources. The measures taken must be implemented effectively and include adequate mechanisms for measuring their impact.

Providing evidence to the US Senate in recent weeks, Facebook founder Mark Zuckerberg highlighted the potential future uses of AI to identify and report illegal, harmful or infringing content:

[977] COM(2017)555 Communication on Tackling Illegal Content Online p. 10 – 11.

[978] COM(2017)555 Communication on Tackling Illegal Content Online p. 11 -13.

'I am optimistic that over a five-to-10-year period we will have AI tools that can get into some of the linguistic nuances of different types of content to be more accurate, to be flagging things to our systems, but today we're just not there on that.'[979]

The MPA has long advocated for an enforcement model under which **all** relevant intermediaries, including ISPs, advertisers and platforms, must take responsibility for ceasing and preventing piracy and the offering of infringing content. We warmly welcome the moves from both the European Commission and the UK Government to recognise this and increase the pressure on platforms to act accordingly. In particular we welcome the recent emphasis by the UK Government to ensure and enforce that activity that is illegal offline is also illegal online.

Action by the UK Government has so far focused on making the internet a safer place for children and adults, primarily by addressing illegal content. For example, the work on age verification being undertaken collaboratively with players from across industry including internet service providers (ISPs) is certainly welcome; however it is focused primarily on content sources which are, in general, authorised and accessible. However this type of work does not fully address the full scope of what is available via the increasing number of online sources via which copyright infringing content (including itself – or accompanied by advertising including - illegal images) may be accessed.

It is therefore vital that the Government pursues a joined up and comprehensive approach to ensuring safety online, recognising that the world of infringing content presents the same level of risk and harm for children and adults as the more traditional online environments, and that platforms should be equally required to take a proactive approach to tackling copyright infringing content, as other illegal and harmful material.

3. How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

Online copyright infringement causes significant economic harm to content creators and all those that work in the creative industries. An IPO report showed that over a three month period in 2017, 18 percent of all digital content consumed in the UK was copyright infringing. During that period, infringing copies of motion pictures and television programmes were accessed by UK users 20 million and 14 million times respectively from illegal online sources.[980] This is clearly of significant concern to the MPA and our member companies. In addition it is these same sources of infringing content that also present considerable consumer safety and child protection concerns. It is clear that platforms must go further to moderate, and take swift action against sites and services that host illegal, harmful or infringing content.

[979] https://qz.com/1249273/facebook-ceo-mark-zuckerberg-says-ai-will-detect-hate-speech-in-5-10-years/

[980] Intellectual Property Office, Online Copyright Infringement Tracker, Wave 7 (March 2017), Table 6.1c. Available at: https://www.gov.uk/government/publications/online-copyright-infringement-tracker-survey-7th-wave

Many cost-effective technologies exist that can be deployed by both large and small platforms – and leveraged by major rightsholders - as key elements of any platform's overall anti-infringement toolkit. For example, Content Recognition Filtering (CRF) systems are effective as they can both recognise content carried by uploaded files and then filter them from publication according to business rules. This ensures that the content is not offered to consumers – and if the offer is made, that any transaction request associated with that content could be stopped. It is important that such a system is flexible, as any given work may be represented by many distinct digital files that differ, for example, in technical recording quality. CRF systems do this via sophisticated analyses of the audio and/or video data contained in the file, a process known as automated content recognition, or by – for example – fingerprint or complex hash-based identification and verification.

Integrating a CRF system into a content site is straightforward and the cost typically involves a one-time setup fee and a usage charge that depends on the volume of files identified. The cost of a CRF solution in relation to site revenue is not fixed and can be, therefore, extremely low. There are several suppliers providing solutions and likewise several examples where this technology has been implemented. Indeed, some have been implemented for years already – and, currently, there are available solutions for SMEs and even individuals as well as solutions that are addressing activity in e.g., the Blockchain and "dark web" environments.

Voluntary Code of Practice for Search

One stream of work to moderate the access to infringing content is a voluntary code of practice that was brokered by Government and agreed in February 2017. This has seen collaboration between internet search providers and the content industry to stop links to infringing content featuring prominently in search results returned to consumers in the UK. The MPA was closely involved in driving the creation of the code and is one of the signatories; however this code took several years of detailed cross industry talks, and is therefore not a suitable model to replicate with other efforts to moderate content. We welcome the recognition of the urgency for action from government with the commitment to consider legislation if no effective voluntary code for platforms, advertisers and marketplaces in not in place by the end of the year.

Under the terms of the voluntary code and since its implementation, rightsholders and search engines have been working together to refine a series of techniques to deliver the objectives of the code, including:

- Automated demotion of infringing content
- Reducing the time between the first identification of such domains and their demotion from top search results
- Encouraging the use of application programming interfaces APIs and the most expedient formatting of infringement notices
- Search optimisation techniques for legitimate sites
- To prevent the generation of autocomplete suggestions which lead consumers towards infringing websites

- Processes to promptly remove advertisements from specific advertisers that link to infringing content

Since its implementation the IPO has been overseeing quarterly cycles of research in order to assess the progress that is being made towards the code's shared objectives as well as specifically considering the extent to which the code is improving the visibility of legitimate content sites. The code provides for ongoing technical consultation, collaboration and detailed information sharing between all the parties to refine the process continually and, where needed, adopt new practices.

To demonstrate the scale of the challenge facing rightsholders, from March to August 2013 MPA members sent takedown notices for almost 12 million links to search engines and more than 13 million links directly to site operators. In the calendar year 2015, MPA members sent notices pertaining to more than 104.2 million links to websites devoted to search and content-hosting. The MPA members received fewer than 210 counter notices during the same time period.

The MPA believes that there is no single answer that will solve the huge challenge of copyright infringement overnight and the code of practice is no different. It has however been an encouraging first step and the MPA welcomed the political emphasis and will behind the creation of the code, and the recognition by search engines that they have a responsibility and a critical role to play in moderating the content they host.

However, this currently agreed voluntary code is not as helpful for audio visual content as for other covered content (predominantly music) – and there remain areas that the code does not address sufficiently. For example, ***removing*** pirate sites from search listings altogether – so called de-indexing or de-listing - is not included even for those illegal sites that are already subject to UK High Court orders requiring ISPs to block access to them.

Going forward, it will be important to keep the metrics for measuring the impact of this first, and definitely helpful (as a starting point), voluntary code under careful review as the Government and industry continue to explore the right mix of tools and policies to meaningfully reduce copyright infringement and access to illegal content via search engines.

In addition to the core shared objective of demoting sites in search listings, there are several other important aspects such as addressing the role of auto-complete; it is important that search engines also work to find solutions on these issues as well.

To address this issue fully will ultimately require action in multiple territories. We hope that this code generates useful insights and techniques that, if effective, could be adopted elsewhere of how online platforms can act to address infringing, illegal or harmful content.

Beyond Search

The MPA believes that there is very little risk of error in the decision to take action against takedown notices referencing copyright infringing, illegal or harmful material.

The standards applied by the MPA member studios to their takedown notices are very robust, resulting in extremely low error rates (0.00003% - 0.0002%). In the very rare situation where an individual wishes to challenge a decision, they should be able to apply to the search engine for the justification for any action, a process which can be referred via a counter notice to the rightsholder in order to clarify in situations of disputed copyright infringement.

4. What role should users play in establishing and maintaining online community standards for content and behaviour?

We believe that rightsholders have a valuable role to play in creating and maintaining a safe online environment. In order for users to be able to play such a role, widespread public education must be undertaken to ensure that consumers fully understand - and are aware of - what is and isn't infringing and illegal content, in order to be able to both moderate their own and others' behaviour and to locate genuine sources.

Consumer education projects such as the Get It Right from a Genuine Site campaign, which brought together content creators (including the MPA) alongside the Government and the main Internet Service Providers has sought to educate the public about the value of and opportunities offered by the sector and, ultimately, to reduce copyright infringement. So far the campaign has used dynamic videos of behind-the-scenes film professionals to demonstrate the amount of time and effort that goes into making films (in order to protect their livelihoods) and has showcased a number of other parts of the content industry to emphasise the importance of consumers accessing legitimate content. Additional components of the campaign then built and deployed processes to send educational emails to ISPs' residential broadband subscribers whose accounts are confirmed to have infringed copyright.

Polling has found that in the two years since the education campaign began, 1 in 4 of the target population (16-50 year olds) have now been exposed to the campaign. Importantly, while piracy among the general population has remained generally static over this period, amongst those exposed to the campaign there has been a drop in 'past month piracy' by 17.5% since the campaign started - and we have seen an equally impressive and statistically significant fall in 'past month piracy' for each wave of research. This demonstrates the impact that awareness and more understanding of the industry and the mechanisms that deliver the content that consumers love can have on those consumers' behaviour, if they know about it.[981]

Building on the consumer campaign it is then vital for the online platforms to ensure users are able to simply report infringing, illegal or harmful content – as well as to identify quickly, and access, ***genuine*** sources of content.

5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

Significant efforts are made to report infringing, illegal and harmful content online. Copyright owners alone spend millions of pounds annually combatting online piracy,

[981] Creative Content UK polling 2017

and countless hours are devoted to identifying this type of content. For example, for notice-sending (addressing files/sources/services directly and/or links to infringing content files), rightsholders must identify the infringing content, notify the platform and follow up on whether the content is removed - an incredibly time consuming and arduous process. In 2015 alone MPA member studios sent notices with respect to more than 46.5 million URLs to hosting sites - and a further 57.7 million URLs to sites devoted to search.

Principally, there needs to be an acknowledgement from online platforms that they should be playing a greater role in reducing the uploading, availability and promotion of known sources of infringing content, digital or physical products via their platforms.

The adoption of the voluntary code of practice for search engines has a been a welcome first step, but there are a number of further measures both search engines and increasing social media and online retail platforms could be taking to ensure online safety.

These include, but are not limited to:

- Creating a set of best practice principles for the effective removal of infringing or harmful links and adverts within a defined time period, and the banning of repeat offenders from social media sites.

- Implementing a requirement for platforms to promote legal content through a range of channels, and ways of reporting infringing content.

- Sellers and promoters of goods that can pose a risk to consumers, e.g. electrical items and toys, could be reported to law enforcement and banned from sites and services.

- Consideration of a consumer education campaign which outlines the risks to the public and particularly children of encountering harmful content on social media sites.

We do not believe that restrictions on the availability online of copyright infringing and illegal content would impact freedom of expression or freedom of information. The production and enjoyment of audio-visual content are significant contributors to the UK economy, and the audio visual sector is a key part of the creative industries which added almost £92bn in GVA to the UK economy in 2016.[982] But the economic contribution is far from the whole story and the audio visual industries are also key contributors to cultural icons, enriching and providing common, shared experiences. Piracy undermines creative endeavour, reducing the value of unique for all those involved in its creation, for personal gain.

6. What information should online platforms provide to users about the use of their personal data?

[982] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/662958/DCMS_Sectors_Economic_Estimates_2016_GVA.pdf

One of the outstanding problems for rightsholders is the ability for users to do business anonymously on the internet in a manner contrary to Article 5 of the E-Commerce Directive. Host services should have an obligation to hold and list valid contact details and a contact person (notice & action agent) as a threshold condition to benefitting from the privileges in the E-Commerce Directive.[983]

Platforms should not be able to claim protection under the safe harbours in the E-Commerce Directive without having listed valid contact details. Further, intermediaries should as part of their societal responsibility refrain from providing services to anonymous actors.

Transparency and Know-Your-Customer (KYC) requirements which exist to prevent crime in the offline world are not universally applied online. Many professionals in regulated industries are under an obligation to know who they are doing business with, while for instance, hosting and domain registrars/registries openly provide their key services to multi-million euro infringing businesses online. Platforms should be required to take greater steps to ensure users are not allowed to anonymously transact business online, in the same way they would not be able to do so offline.

7. In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

While we urge platforms to play a greater role in reducing the promotion of known sources of infringing content, digital or physical products through technological solutions, the use of these solutions must be implemented in an effective manner, ensuring that they are measured and monitored to be continuously (and, hopefully, increasingly) effective.

Such measurement and monitoring is only possible if platforms are transparent in their implementation of the technology and provide rightsholders with accurate and regular data. Rightsholders can then work with platforms to improve the effectiveness of the technology.

The MPA therefore believes that platforms should make a greater effort to ensure that service providers (such as operators of sites and services) that use their platforms identify themselves online and can be contacted. Such transparency is a long standing cornerstone in all forms of commerce, and Article 5 of the E-Commerce Directive (ECD) embodies this principle in the online world by requiring information society service providers to clearly indicate their identity. However, illegitimate service providers routinely ignore Article 5 ECD with impunity, wilfully hiding their identity for reasons including: to infect consumers' computers with malware, commit fraud, infringe rights of privacy or property, avoid paying taxes, or otherwise violate the law naturally prefer to remain anonymous.

The MPA's expertise in this area specifically pertains to websites that engage in commercial-scale infringement of copyright in film and TV programmes. MPA's analysis of a group of 122 sites of concern in that regard in Europe between 2013 and

[983] (cf., section 512(c) of the DMCA on the obligation to designate a DMCA agent as a prerequisite to safe harbour protection). United States Digital Millennium Copyright Act, http://www.copyright.gov/title17/92chap5.html#512

2015 indicates that **only a small minority (13%) of suspect sites listed contact information that appeared likely to be accurate in publicly accessible WHOIS databases, while the other 87% hid their identities.** Most of the sites MPA analysed (71%) were hosted via publicly available anonymisation services, such as Whoisguard Inc. and Privacy Protection Service Inc., which advertise themselves as a way for individuals registering domain names to protect themselves from spammers. In the case of commercial information society services providers, however, use of such a service tends to indicate that the service provider is choosing not to comply with Article 5 ECD.

The policy implications of widespread non-compliance with Article 5 are serious, particularly but not exclusively for rights holders. While the data above is focused on the audio-visual sector, where our experience lies and the problem is acute as to illegal sites, investigations by EU Member State consumer protection authorities have found the problem to exist in other areas as well. The ability to operate anonymously online undermines the rule of law in fields such as consumer protection, privacy, and taxation – to name just a few – and enables online criminal activity.

This need for transparency is compounded by the potential loss of access to the public directory, also known as the WHOIS database, which is coordinated by The Internet Corporation for Assigned Names and Numbers (ICANN). WHOIS data gives information about ownership of a domain name on the internet, and indicates how best to contact the owner/s. However, after the pending EU General Data Protection Regulation (GDPR) rules come into force, some or all of the key data in this public directory, also known as the WHOIS database may not be accessible to even qualified representatives of Law Enforcement agencies.

Law enforcement, child protection organisations, anti-human trafficking organisations, cybersecurity firms, health and safety organisations, and intellectual property rights owners, rely upon WHOIS to investigate and combat a wide range of illegal and abusive online activity. According to the European Commission, "WHOIS lookup is the first step in many cases involving abuse of networked resources."

ICANN has proposed recently changes to the publication of WHOIS data that will severely limit, and in some cases eliminate, access to this important information. If the GDPR is applied to WHOIS in a way that makes most of this contact information disappear from public access, and makes it difficult for legitimate parties to obtain it, it is likely that illegal and abusive activity online and offline will increase and public welfare and safety will be put at risk. We also believe that the Information Commissioners Office has not yet raised any concern about or objection to ICANN's proposal.

May 2018

Dr Victoria Nash, Professor Christopher Marsden, and Professor Lorna Woods – oral evidence (QQ 1-11)

Transcript to be found under Professor Christopher Marsden

National Crime Agency Internet Watch Foundation, Metropolitan Police and National Police Chief's Council – oral evidence (QQ 35-43)

Transcript to be found under Internet Watch Foundation

National Police Chief’s Council, Internet Watch Foundation, Metropolitan Police and National Crime Agency – oral evidence (QQ 35-43)

Transcript to be found under Internet Watch Foundation

Professor John Naughton and Jennifer Cobbe, Trustworthy Technologies Strategic Research Initiative, University of Cambridge – written evidence (IRN0031)

Written evidence to be found under Jennifer Cobbe

Professor John Naughton and Dr Ewa Luger – oral evidence (QQ 93-102)

Transcript to be found under Dr Ewa Luger

News Media Association – written evidence (IRN0059)

The News Media Association (NMA) is the voice of national, regional and local news media organisations in the UK – a £5 billion sector read by 48 million adults every month in print and online. The NMA exists to promote the interests of news media publishers to Government, regulatory authorities, industry bodies and other organisations whose work affects the industry. We welcome this inquiry into the state of the internet and what, if anything should be done in either the regulatory or the self-regulatory fields of the online world. This field is constantly developing, and so great care must be taken not to put in place regulations that may have unintended consequences in the face of news media companies' business models adapting to technological developments. This may be particularly problematic when attempting to define categories of businesses, such as platforms, and concepts such as fake news.

Given the challenges that the online world can pose – it provides anonymity for the purposes of hate speech and crime, and reduces the efficacy of traditional jurisdictional borders – the appeal of introducing regulation is understandable. However, "internet regulation" is a misleading and dangerous mirage. The internet is so fluid and diverse that any system of online content regulation would not be fit for purpose - unable to provide for the nuances in current and future online activity. It would inevitably result in heavy handed and ill-fitting rules that damage individual privacy, freedom of expression, and the entrepreneurial drive that has secured the internet's position in modern society. Instead of regulating the internet itself, the Government should therefore address the business models that generate problems, the most notable of which are online platforms. The NMA would like to reiterate points that it has made in the past, both to this Committee and more widely, that the most pressing issue online is the need for a review of competition regulation, with particular reference to the tech companies' exploitation of their dominant positions. The NMA has been calling for the CMA Ofcom and ICO to urgently investigate the digital advertising supply chain, the dominance of the tech platforms and their impact on consumers, advertisers and other media players, and put in place measures to address the problems.

Need for Competition Reform

We refer the Committee to the NMA's prior submissions to this Committee on digital advertising,[984] and to the Commons fake news inquiry,[985] as well as the oral evidence[986] submitted by the NMA on these issues. Review and reform of the regulatory regime to ensure fair and sustainable competition to address problems created by the dominance of tech companies is now necessary. The NMA was a signatory to an open letter[987] sent to the CEO of Google in April 2018 from organisations representing publishers in response to Google's approach to the GDPR. Google has used the requirements imposed by the GDPR as an opportunity to

[984] https://www.parliament.uk/hlcomms-advertising-industry

[985] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/ culture-media-and-sport-committee/fake-news/written/48244.html

[986] https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/inquiries/parliament-2017/fake-news-17-19/publications/

[987] Open letter to Google: http://www.newsmediauk.org/write/MediaUploads/PDF%20Docs/DCN_Letter_to_Google_re_GDPR_Terms.pdf

strengthen its already monopolistic position. It announced its plans the month before GDPR is due to come into force, leaving no time for publishers or other online actors to consider or discuss how this implementation would impact the online ecosystem, or whether they allow businesses that interact with Google any sort of flexibility on the terms in which they do so. This shows the problems created by exploitation of Google's dominant market position, and further emphasises the need for the CMA and the ICO to investigate and address the impact of Google and other tech companies on the online ecosystem, and highlights the need for the Government to ensure that regulations are not exploited by these companies as opportunities to increase their stranglehold on the digital market. This is bolstered by the BEIS Green Paper[988] that is calling for views on how to change regulatory and competition regimes to meet emerging challenges including the growth of fast-moving digital markets, and whether the enforcement regime gives the CMA and regulators the tools that they need to tackle anti-competitive behaviour and promote competition.

Increased Responsibility of Platforms

A regulatory review of the status of the tech platforms to determine whether they should be categorised as publishers rather than mere "conduit", and what additional responsibilities that they should bear for the content that they host, is necessary. This should be done without imposing new restrictions upon news media publishers, or allowing tech platforms to seek to shift liability, costs and regulatory burdens to news media publishers and other online players. Platforms exert significant influence the basis of information gathered about individual users, the impact of which could not be in sharper focus following the revelations about Cambridge Analytica. They exercise a huge amount of control over what users see, both in terms of content and advertising. Much greater transparency and accountability are needed. Platforms must be clear about information they use, how their algorithms prioritise content, and how third parties are allowed to use this information.

It is imperative that platforms are held to a level of responsibility that reflects both their financial dominance and the detrimental effect that this dominance has on other sectors. In 2017, Facebook and Google combined claimed more than half of the UK's digital advertising revenue, and this is forecasting to keep increasing.[989] This domination of the UK online market means that content creation industries like the news media are beholden to the very platforms that are threatening their viability. Publishers invest £97 million in digital services[990] and drive over 900 million social media interactions a year.[991] Nearly half (47 per cent)[992] of all engagements with UK websites on social media over the past year sourced content from UK news brands and eight of the top 10 most shared UK websites on social media were UK news media sites[993]. At the same time, fake news sites and other harmful content online are fuelled

[988] BEIS, Modernising Consumer Markets: Green Paper https://www.gov.uk/government/consultations/consumer-green-paper-modernising-consumer-markets

[989] eMarketer, Digital Duopoly to Remain Dominant in UK Ad Racehttps://www.emarketer.com/Article/Digital-Duopoly-Remain-Dominant-UK-Ad-Race/1016481

[990] NMA Deloitte Report, 'UK News Media: Engine of Original News Content and Democracy,' 2016 http://www.newsmediauk.org/write/MediaUploads/In%20the%20Spotlight/NMA%20Economic%20Report/Final_Report_News_Media_Economic_Impact_Study.pdf

[991] Newswhip Analysis 2016 http://www.newsworks.org.uk/Opinion/newswhip-data-newsbrands-rack-up-901-million-social-media-interactions-in-2016/161765

[992] NMA Newswhip Research, 2017 http://www.newsmediauk.org/News/uk-news-media-journalism-powers-social-networks/181674

[993] NMA Newswhip Research, 2017

by digital advertising, to the benefit of tech platforms, agencies and other intermediaries, but to the detriment of society, advertisers and the publishers of genuine news. It has been reported that even government advertising has unknowingly been served up on highly inappropriate content as a result of blind programmatic ad buying practices. Reviewing online advertising is a practical way that the government could address issues of market dominance and illegal content using principles of competition regulation without endangering free expression. A rebalancing of the business model of the free to access internet would allow revenues to reflect the investment into content and the societal value of independent journalism, in line with the Government's earlier pledge to "ensure content creators are appropriately rewarded for the content that they make available online."

Protecting against Risks to News Media

Conversely, in seeking to better regulate the technology companies, it is vital that new restrictions and liabilities are not placed on news media publishers, through EU or UK legislative or co-regulatory or voluntary controls. News publishers are already subject to a myriad of legal controls over their editorial and advertising operations. They voluntarily fund and adhere to the independent editorial and advertising industry self-regulatory systems upheld by IPSO and the ASA. Payment by the major tech companies, internet and social media companies of a proportionate and full contribution to the financing of the advertising self-regulatory system reflecting the size of their advertising revenue and share of the advertising market is needed to protect a fair online environment that respects the role of the independent news media in democracy. Any proposals should be drafted with particular care not to restrict or inhibit news publishers as they adapt their business models to serve an increasingly online audience.

Protection of Intellectual Property Rights

Maintenance of a strong intellectual property regime should be a priority in any review on online regulation. UK news publishers' IP rights and remuneration derived from them, without dilution, should be protected under UK and overseas IP regimes. This includes promotion of an improved Publisher's Right to benefit UK news publishers and the prevention of a detrimental version. (IP issues are also relevant to external funding and commercial relationships.) The protection and maintenance of current legal deposit regime that does not permit commercial exploitation by libraries or anyone other than the publisher should also be prioritised.

The NMA would be very happy to discuss any of the above issues in more detail.

11 May 2018

NINSO (The Northumbria Internet & Society Research Interest Group)[994] – written evidence (IRN0035)

Summary	
1.	• An assessment of existing laws and regulatory approaches should be undertaken. Existing regulation should then be amended, taking an evidence-based approach • There should be consideration of online norms and the role of the law in shaping norms • Education must be a key consideration
2.	• A tailored approach should be applied with reference to size, resources, technical means and content • Determination of liability should go beyond the 'notice and takedown' mechanism • A platform should be liable where it has knowledge of unlawful content or the technical means to ensure legality
3.	• Moderation processes are generally opaque • There are limited options available for individuals who disagree with a platform's decision • Alternative systems include an online optional dispute resolution platform • A tailored approach to platforms is required based on size and resources
4.	• Users should be responsibilised; education should be integrated as part of the online user experience • Users could establish and maintain online norms • Large organisations could consider introducing a review panel composed of independent users
5.	• The right to privacy should also be protected by any measures introduced • Measures should be appropriate to the resources of the platform • Additional safeguards should be introduced to protect children • Education must be a key consideration
6.	• A summary of key information should be provided followed by a detailed explanation • The method of informing users is of equal importance • Platforms must ensure a level of clarity sufficient for users to make a clear choice • The issues of power imbalance and genuine choice should be given consideration • Education must, again, be a key consideration
7.	• Adherence to principles of fairness, accountability, transparency, privacy and user-friendliness is required • The algorithm should be disclosed in full in certain circumstances
8.	• The issue of power imbalance between the user and the platform should be considered • A holistic approach should be applied
9.	• The existing jurisdictional problem of fragmentation of internet laws is likely to be worsened • The UK cannot afford a fundamental divergence from the EU position on matters including cross border transfer, geo-blocking and portability of digital content • Participation in relevant EU initiatives should be considered

[994] NINSO (The Northumbria Internet & Society Research Interest Group) is multidisciplinary enterprise consisting of researchers from law, business, social sciences, computer science, engineering, and architecture, with a research interest at the intersection of internet and society. For more information please see: https://www.northumbria.ac.uk/about-us/academic-departments/northumbria-law-school/law-research/ninso-the-northumbria-internet-and-society-research-interest-group/

NINSO (The Northumbria Internet & Society Research Interest Group) – written evidence (IRN0035)

1. **Is there a need to introduce specific regulation for the internet? Is it desirable or possible?**

1.1. The scope of this question appears to be very broad. It is considered noteworthy that the question asks whether it is necessary to introduce specific regulation for the 'internet' whilst subsequent questions refer to 'online platforms'. If the intention is to regulate 'the internet' then this is clearly more complex than regulating a specific part of the internet; very different issues are raised when one considers the different types of online platforms now available (for example: large social media entities such as Facebook, Instagram and Snapchat; sites which offer opportunities to buy online including Amazon, eBay; online gaming sites; dating applications; discussion forums, websites and social media pages operated by individuals to allow other members of a sporting club or village to gain information about interests of specific relevance to that group). There is no 'one size fits all' answer that can be applied to all of these platforms and a tailored approach is necessary.

1.2. In addition, the scope of any regulation should be considered in order to ensure a more focused application. In 2014/5 the HL Communications Committee report published on social media and criminal offences considered, at that time, that the criminal law was generally appropriate for the prosecution of offences committed using social media. It is therefore queried whether the intended scope of the current call for evidence is focused on civil regulation. This would make the project more manageable and seems sensible, though consideration should be given to the intended approach (e.g. from the standpoint of ecommerce or for the protection of individuals, or both).

1.3. In answer to the question of whether it is desirable or possible to regulate the internet, it is submitted that the internet is already heavily regulated in the UK where there exists, for example, the ICO in relation to online data protection and privacy; Ofcom in respect of online streaming services and ASA with regard to online advertising standards. The first step should be to collect all existing laws and regulations and assess whether they are consistent. Secondly, one should try and take a holistic, evidence-based approach and amend existing laws accordingly.

1.4. Whilst regulation should be kept to a minimum, not all regulation stifles innovation. Regulation is fundamental when it is industry practice to violate fundamental rights by contractual means (e.g. privacy and consumer protection). More evidence is needed to assess which of the following approaches is the ideal one: regulation, co-regulation, or self-regulation. In regulating, one should keep in mind the inherent jurisdictional problem; therefore, emphasis should be given to private international law and conventional initiatives.

1.5. Whilst it may be appropriate to regulate some aspects, it may be less appropriate to impose strict rules in respect of others. Two particular issues for consideration are set out as follows:

1.5.1. *How information is used by online platforms and those who offer services via the internet***.**

It is arguable that this is an area which both should and could be subject to regulation. Whilst arguably these platforms are already subject to data protection regulation, the recent issues with Facebook and Cambridge Analytica suggest there is scope for greater regulation of the use of individual's personal data. One particularly significant issue that has been identified is that there is a substantial power imbalance between users and the operators of online platforms. Users frequently have no capacity to moderate terms but instead have the 'choice' of accepting all terms (which might include giving away significant amounts of personal data) or simply not using the service. This is not providing a real choice.   Alternative models are explored below at 6.3.

1.5.2. *How the rights of individuals to exercise their rights to freedom of expression are balanced with the rights of individuals whose information is posted online, particularly where that information is posted online without their knowledge or consent*.

The heavy censorship of countries, such as China and Bahrain, is not considered desirable. However, it is suggested that consideration does need to be given to ensuring that there is effective regulation in place to enable individuals to challenge a breach of their right to privacy. There are potentially difficulties in regulating the speech of individuals given the global nature of the internet. However, the case of PJS v Newsgroup Newspapers (2016) suggests that to some extent legal regulation of the internet can be effective even in the face of worldwide disclosures.[995] The bigger issue here, perhaps, is not, however, a lack of regulation. As noted above data protection regulation already exists. As the Information Commissioner has made clear, however, they will not consider complaints made by individuals against other individuals who have posted information online in a personal capacity. This is at odds with the approach in many other European countries.[996] It is, however, a pragmatic response to limited resources.[997] By contrast,

[995] *PJS v Newsgroup Newspapers* [2016] UKSC 26

[996] See: David Erdos 'Beyond having a domestic: Regulatory interpretation of European Data Protection Law and Individual Publication' Computer Law and Security Review (2017) 33(3) 275-297

[997] See: ICO, Social Networking and Online Forums – When does the DPA apply? https://ico.org.uk/media/for-organisations/documents/1600/social-networking-and-online-forums-dpa-guidance.pdf [accessed 4 May 2018]; and
The Law Society and others v Rick Kordowski [2011] EWHC 3185 (QB))

recent empirical research, whereby a group of 45 parents were asked about their knowledge and understanding of the law and how it could be used to protect their family's privacy suggests that many individuals already believe that regulations exist which would allow them to request the deletion of online posts which they have not consented to.

1.6. Reference is made in the call to the comments in the Government's Internet Safety Strategy that 'what is unacceptable offline should be unacceptable online'. This is not disputed. What needs to be considered, however, is whether, in fact, in some situations, a greater level of regulation is needed in the online sphere than in the offline sphere. In interviews with parents, a significant number of parents expressed concern that the impact of online disclosure is significantly greater and longer lasting than offline disclosure. It was clear from these interviews that what some individuals find unacceptable online they may in fact consider to be acceptable (or treat as mere gossip) offline. By contrast, however, some individuals, who are regular users of online platforms may be happier for information to be disclosed online. The extent of technology use, the extent to which users trust those with whom they associate online, age of users, anonymity of platforms etc. are all relevant to individuals' views. So many people use the internet in so many different ways it may be difficult to establish a 'norm'.

1.7. Before any decision can be made about regulation, therefore, careful consideration needs to be given to what online 'norms' are and the role that the law plays in shaping norms. As noted above many individuals believe that they should be able to control what information is posted about them online; they understand that they already have a right to redress where posts are made without consent. There is therefore an issue not only of regulation here but also of providing guidance to individuals and managing expectations.

1.8. It is submitted that one of the key concerns should be education and raising of awareness so that individuals have a clearer understanding of the control over personal data and possible redress available (especially in light of the GDPR). This is considered in more detail below at 6.

1.9. The importance of education also extends to the organisations which process the data, to which education on safe working practices, existing laws on privacy, freedoms, crime etc. should be provided. This could also be combined with a code of practice guided by a set of principles that include respecting and using personal data appropriately, making sure people understand the rules that apply to them when they're online and putting in place protections to keep people safe online. This should also ultimately contribute to a system of compliance based on the key concept of 'privacy by design'.

2. **What should the legal liability of online platforms be for the content that they host?**

2.1. Again, a 'one size fits all' solution would not be suitable for every platform and a tailored approach would be more appropriate taking into account the size, technical means and resources of the platform. A similarly tailored approach should also be applied to different content, with more extreme content necessitating more extreme measures. Online platforms should be liable not merely for illegal contact but more generally should be liable for unlawful content i.e. posts that defame, breach privacy laws including the provisions of the GDPR, result in nuisance of harassment and the violation of copyright.

2.2. Determination of liability should go beyond the 'notice and takedown' mechanism; a platform should be liable if it has knowledge of the unlawful content or it has the technical means and resources to ensure the legality of the activities carried out on the platform while striking a balance between the different interests involved, including freedom of expression. Platforms which de facto or de jure monitor users cannot invoke immunity (so-called safe harbours).

2.3. If content is from third party sites, then it should not be the responsibility of the content provider platform; accountability should lie squarely on those generating the content in the first instance. As mentioned above, however, if content provider is aware of the inappropriate content then they should have the responsibility of removing content.

2.4. Consideration should be given to issues regarding policing of sites, reduction in privacy, freedom of expression and information.[998] Moreover, there should also be consideration of whether contract law at its current state is sufficient to establish liability between content providers, online platform/interface, host, ISP, site and app developers. Potential standardization of terms of service for ISPs and search engines used within a jurisdiction could provide a consistent and transparent system in disclosing information held/monitored and how the site will process these. The GDPR will be of value in this regard.

3. **How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?**

3.1. At present, online platforms are often over-effective when it comes to intellectual property infringement and non-effective when it comes to other forms of content, for example in relation to terrorism.

3.2. Furthermore, moderation is often opaque and one of the real issues that users face is a lack of guidance as to what policies online platforms operate. Even when platforms do provide an accessible policy it is not helpful to the ordinary

[998] See also E-Commerce Directive Art 12, 13, 14;
Digital Content Directive; Digital Single Market; European E-Commerce Reforms 2018

individual and indeed may be considered misleading. As an example of this, see Facebook's community standards page which states that 'you may not publish the personal information of others without their consent.'[999] Many individuals do, of course, publish other individuals' personal information without consent, for example when posting photographs. Facebook states elsewhere that it 'provides people with ways to report photos and videos that they believe to be in violation of their privacy rights. We'll remove photos and videos that you report as unauthorized if this is required by relevant privacy laws in your country.'[1000] Since few people know what the actual legal position is, it will not be clear to the average individual whether or not they have a right to seek removal of a photograph and such a statement is not, therefore helpful. Transparency is key in this matter; however, careful consideration should be given to how 'transparency' is defined, covering what is meant by 'effective' and 'fair' in this context.

3.3. In any event, whilst in principle online dissemination of an individual's personal information without consent might be considered to breach data protection provisions (which will of course emphasise the importance of consent still further from 25 May 2018) it appears that Facebook's position on removal of posts is far more limited, and focuses on matters such as hate speech, incitement of terrorism, but not a photo of mundane activities in ordinary life[1001]. This is perhaps understandable given the EU position as detailed in the European Commission's Recommendation of 1.3.2018 on measures to effectively tackle illegal content online[1002] and the Information Commissioner's current approach to the DPA and social media as detailed above at 1.5.2.

3.4. There are of course issues with online platforms 'self-policing'. At present there are limited options for individuals who disagree with the decision of a social media giant unless they have the financial capacity to bring court proceedings. In terms of remedies, an online optional dispute resolution platform managed by a trusted independent third party should be available. This should not replace judicial redress. It should be recognised that most of the decisions taken in this context fall under the GDPR, Article 22. However, it is crucial to make sure that remedies are available also beyond the GDPR, e.g. when no personal data is processed or if the decision is not solely automated. A task force with members of the national Data Protection Authority and of the Consumer Protection Authorities should oversee this (though again the current stance of the ICO to the Data Protection Act and social media poses problems). A further alternative might be to adopt the suggestion made by the

[999] Facebook Community Standards https://www.facebook.com/communitystandards/ [accessed 4 May 2018]

[1000] Facebook Image Privacy Rights https://www.facebook.com/help/428478523862899 [accessed 4 May 2018]

[1001] See for example: Revealed: Facebook's internal rulebook on sex, terrorism and violence https://www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence [accessed 4 May 2018]

[1002] Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online (C(2018) 1177)

Children’s Commissioner to put in place a children’s digital ombudsman, to mediate between under 18s and social media companies, and/or to put in place a digital ombudsman to support any individual.[1003]

3.5. It must not be forgotten, of course, that there are many different types of online platforms including smaller platforms, for example websites operated by sporting groups or from community interest, which will also operate their own moderation policies. Online platforms vary widely in how they have been developed, their functionality and what their objectives are, and each have various business models for operation. Given that such groups will rarely be able to benefit from the legal advice available to large corporations, a tailored approach to regulation or at least guidance for such groups would undoubtedly be helpful.

3.6. The agenda should be evidence-based and research-informed; therefore, academics should play an important role and should be consulted.

4. **What role should users play in establishing and maintaining online community standards for content and behaviour?**

4.1. Users should be reasonably responsibilised. Long, unfair, and opaque privacy policies and usage guidelines are not a good way to achieve this. Education and advice should become integrated as part of the online user experience reminding users of the privacy options available. Users should also be held responsible and accountable to adhere to age restrictions, publishing content that is appropriate/inappropriate such as photographs, messages that are libellous, offensive, illegal, damage to reputation, bullying and humiliating.

4.2. In addition, it might be seen as appropriate for users to establish and maintain online community standards (acting together as part of a responsible community). The difficulty in the online sphere is that we have yet to see the establishment of norms of disclosure i.e. what it is appropriate to disclose online, as discussed above at 1.7.

4.3. There is again a distinction to be made between the establishment of standards on platforms operated by large corporate entities and small sites. Even on smaller sites, however, significant differences of opinion are often evident between the moderators of such sites. On bigger sites one possibility that might be considered could be a review panel composed of independent users, who vote and report on decisions which have been appealed by a user of the site. Consideration would need to be given to the definition of the users appointed, the method of appointment and the steps that should be introduced to ensure that membership registration is a legitimate attempt to join the site

[1003] Growing Up Digital, A Report of the Growing Up Digital Taskforce (2017) https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/Growing-Up-Digital-Taskforce-Report-January-2017_0.pdf [accessed 4 May 2018] and not merely an attempt to exert influence over standards and their enforcement. Matters such as diversity, bias, confidentiality and relevance should also feed into the discussion.

5. **What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?**

5.1. This is a very broad question. Online safety and freedom of information are very different issues and would require very different measures. Furthermore, it is interesting that this question focuses on freedom of expression and freedom of information yet makes no reference to rights to privacy. Rights to privacy should be considered alongside and recognised to be of the same fundamental importance as rights to freedom of expression.

5.2. Moreover, it is important that measures differ depending on the resources of the platform. Regulatory initiatives should be taken bearing in mind the risks of over-protection of certain interests (e.g. IP holders). In no instance, however, should platforms be allowed to invoke immunities based on the lack of knowledge if they carry out forms of private surveillance e.g. for advertising purposes. Preventive measures should be a last resort and they should have a sound empirical basis.

5.3. As noted above specific consideration needs to be given to the rights and vulnerabilities of children, who would benefit from the support of their own digital ombudsman. It is suggested, however, that additional consideration needs to be given by large platforms to whether a user is a child and indeed whether a post relates to a child. A duty of care might for example be imposed upon large organisations with significant resources, such as Facebook, Instagram, Snapchat, Twitter, with, for example, privacy settings being set to respect privacy, as a default, when images or information relate to young children with a limitation also imposed on the extent to which information and images relating to that child can be copied, re-contextualised or disseminated further.

5.4. An alternative measure, which may be easier to implement, could be to incorporate a system whereby a user receives a pop-up message each time information featuring an individual’s image is shared, which informs and reminds the user of the rights, restrictions and obligations in relation to data privacy. This method also strikes a balance between privacy and freedom of expression through the use of ‘nudges’ rather than more severe methods such as filtering, censoring or blocking of content.

5.5. Clearly, the importance of educating users should be integral when incorporating the concept of privacy by design.

6. **What information should online platforms provide to users about the use of their personal data?**

6.1. It is important that individuals are provided with a summary of the type of data collected, the purposes for which every type of data is collected, how the data is processed and the third parties with whom the data is shared. The summary should be followed by a thorough explanation of all the data collected in compliance with the GDPR. Separate information is required for sensitive personal information, for example data regarding religious beliefs. The explanation should also describe the data which is provided by the individual directly, collected through use of the platform and inferred through further profiling and automated decision making.

6.2. It is equally as important, however, to consider how the information is delivered to individuals. In line with the requirement for privacy by design, the terms of service and privacy policies must be clear and easy to understand. Videos and infographics are goods ways to convey complex information such as this. The keywords should be in bold. The text should be readable, i.e. coefficient 8 Flesch-Kincaid. This policy should also comply with the Unfair Terms regime. Ultimately, the information should be delivered with a level of clarity that is sufficient to enable users to make an informed choice.

6.3. The concept of choice, as discussed above at 1.5.1 is an important issue which needs to be addressed. It is arguable whether users have a genuine choice as to whether to consent to processing given that, oftentimes, users are faced with the option of providing consent (which might include giving away significant amounts of personal data) or simply not being permitted to access the service, with no capacity to moderate the terms. Alternative models include:

i. no data collection beyond collection of data needed for the user to receive the service;
ii. default position is no data collection but data collection is possible with the user's explicit, valid, fully informed consent;
iii. data collection is possible only upon payment to the individual; or
iv. no data collection upon payment of a premium, free service individuals agree to provide data (this is not a model we support since it disadvantages the marginalised.

6.4. In any event more emphasis should again be placed on education and raising awareness of rights in relation to data minimisation. Again, privacy by design is an important principle in this regard.

7. **In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?**

7.1. Online platforms must adhere to principles of fairness, accountability, transparency, privacy and user-friendliness in relation to how decisions are made and the reasoning behind decisions. Article 22 of the GDPR can go to some lengths to determine these but not completely, particularly if machines are capable of self-learning.

7.2. There are also circumstances where a technical document which includes the algorithm used and a mere explanation of the logic in mathematical terms will not arguably meet the legal requirement under Article 22 of the GDPR. For example, in the context of court proceedings which are subject to obligations of confidentiality, platforms should disclose the algorithms themselves if they are used to make decisions affecting their users, to allow users to obtain expert evidence and therefore ensure access to a fair trial. The GDPR should be interpreted as the disclosure of the algorithm with an explanation in layman's terms about the rationale of the decision and criteria relied upon.[1004]

7.3. Algorithms should also be auditable and audited frequently by an independent body.

8. **What is the impact of the dominance of a small number of online platforms in certain online markets?**

8.1. The impact can be devastating. This again relates to the significant power imbalance between the user and the large organisation, where individuals are not able to negotiate the terms and there is in effect no real 'choice' at all. This issue should be considered in combination with the risk of 'lock-in effect' resulting from the disproportionate level of power in the hands of the oligarchy of online platforms whose business models rely heavily on the valuable currency of big data.

8.2. A holistic approach to personal data and big data, which also takes into account competition law, is necessary.

9. **What effect will the United Kingdom leaving the European Union have on the regulation of the internet?**

9.1. This is a question that can only realistically be answered once it is clear what shape Brexit will take and what steps the Government will take to ensure ongoing co-operation with Europe.

9.2. In general, there is a real risk that leaving the EU will worsen the existing jurisdictional problem of fragmentation of internet laws, across IPR, ecommerce, cyber security, and competition for UK businesses.

9.3. It is submitted that the UK cannot afford to have a fundamental divergence to the EU and a solution on cross-border data transfers, geo-blocking and on the portability of digital content must be a top priority.

[1004] Guido Noto La Diega, 'Against the Dehumanisation of Decision-Making. Algorithmic decisions at the crossroads of Intellectual Property, Data Protection, and Freedom of Information' (2018) 9(3) JIPITEC 1

9.4. Consideration should also be given to whether the UK will be able to participate in relevant EU initiatives, for example the Cloud Computing initiative and DSM.

10 May 2018

Nominet – written evidence (IRN0053)

Nominet is driven by a commitment to use technology to improve connectivity, security and inclusivity online. For 20 years, Nominet has run the .UK internet infrastructure, developing an expertise in the Domain Name System (DNS) that now underpins sophisticated network analytics used by governments and enterprises to mitigate cyber threats. The company provides registry services for top level domains, and is exploring applications for a range of emerging technologies. A profit with a purpose company, Nominet supports initiatives that contribute to a vibrant digital future.

We welcome the opportunity to respond to the Select Committee's public call for evidence on the question of regulation of the internet should be improved.

Regulation

The UK has one of the world's leading digital economies, this success has been built on the foundations of a free and open internet which enables freedom of expression subject to the rule of law. The internet operates within existing legal frameworks, the e-Commerce Directive is a good example of pragmatic harmonized rules based on the most effective regulation rather than the strictest.

We recognise that there are certain misgivings about how the internet, and behaviours on the internet, continue to develop. The difficulty in tackling these issues through additional regulation lies not only in complex cross-border jurisdictional issues, but also the fact that the internet is a complicated technical ecosystem which is constantly evolving and finding new forms of innovation. New technologies are continually emerging which will fundamentally reshape many existing day-to-day activities and the business models built around them. This can already be witnessed in the nascent autonomous vehicles, Internet of Things (IoT), and commercial drones markets. Clearly this equipment will be reliant on highly reliable connectivity to the internet and it is important that any attempt to regulate internet activities does not inadvertently stifle this type of innovation. Given the difficulties in 'future-proofing' legislation, it may not always be the most effective means of addressing concerns. Any regulatory interventions that are introduced should be targeted at clear problems so that focused practical outcomes are achieved and unintended consequences avoided.

It may be worth exploring more flexible measures such as the role of self-regulation which may be able to adapt to future developments much more effectively than the blunt tool that is legislation. A useful demonstration of how self-regulation can be effective is from September 2013 when Nominet aided an independently chaired review by former CPS Director of Public Prosecutions Lord Macdonald QC of our registration policy for .uk domain names. The scope of the review focused on whether there should be restrictions on the words and expressions permitted in .uk domain name registrations. During the course of the review a wide range of stakeholders were able to contribute their thoughts on the issue as part of the evidence gathering. In January 2014 the company adopted the recommendations to restrict the registration of domain names that relate to a serious sexual offence if there is no reasonable use for that domain name. At the same time, we revised our terms and conditions to expressly prohibit any .UK domains being used to carry out criminal activity. It means that Nominet can quickly suspend a domain name when alerted to its use for criminal activity by the police or other law enforcement agencies, such as National Crime Agency, Child Exploitation and Online Protection Centre (CEOP) or the Medicines and Healthcare Products Regulatory Agency (MHRA).

Content Issues

The Domain Name System (DNS) came in to being in nineteen eighties as a mechanism for providing user-friendly addresses for technical resources across the rapidly growing internet. The protocol was built to sit as part of the broader internet 'stack' and has evolved to become the default signposting and navigation method for web, email and machine-to-machine communication on the internet. Nominet is responsible for the management of the .UK DNS infrastructure which currently has over 12 million .UK domain names registered, our servers handle more than 6 billion requests every day.

It is important to note that a domain name in itself does not constitute "content", the domain name is merely an internet signpost which allow websites and emails to have an easy to remember address like "nominet.co.uk" rather than an "IP address" which is a string of number and letters between 4 and 32 characters long. As such, suspending a domain name would not stop a website being accessible as a website can have multiple domain names and can always be accessed via its IP address.

In those instances where a .UK domain name is being used in connection with fraud or other criminality we have formal policies and processes in place which facilitate the effective cooperation with Law Enforcement Agencies (LEAs) and Trading Standards. If a query is received from one of these bodies it is handled by a dedicated support team in Nominet who are able to rapidly suspend a domain name if necessary. We cannot and do not attempt to directly police the content of websites using our domain names. However, if a domain name signals criminal content and is brought to our attention we will refer it to the appropriate LEA for further action. Our most recent report covering the 12 months to October 2017 shows that 16,632 domain names were suspended for criminal activity which represents around 0.14% of the more than 12 million .UK domains currently registered.

Nominet is a long-standing member of the Internet Watch Foundation (IWF) and we have procedures in place to immediately suspend any domain name identified by the IWF as hosting child sexual abuse material. The IWF is an excellent example of how the internet industry, police, governments and charities come together to form a partnership in order to combat child sexual abuse images online. The organisation is widely recognised internationally as a leading model of self-regulation.

Internet Governance

Nominet was established in 1996 at a time when the internet landscape looked very different. As one of the long-standing country code registries, the company has been deeply involved in both national and international policy development relating to the internet and how the underlying internet infrastructure is organised and operated.

We are strong advocates of the multi-stakeholder model of internet governance and have worked closely with the UK Government over the years to preserve and strengthen this approach to guard against the risk of inter-governmental treaties which could fundamentally alter the internet we recognise and enjoy today.

Our participation in the on-going development of internet governance has mainly been via the UK's Multi-stakeholder Government Advisory Group (MAGIG), ICANN's Country Code Name Supporting Organisation (ccNSO) and the UN-backed Internet Governance Forum. We were also an active member of the multi-stakeholder Working Group which dealt with the successful IANA Transition from the US Government to Public Technical Identifiers (PTI), an affiliate of ICANN, in 2016. This was an important issue for us as it concerned the accountability, transparency, and oversight of .UK. PTI is now responsible for the operational aspects of coordinating the Internet's unique identifiers and maintaining the trust of the community to provide these services in an unbiased, responsible and effective manner.

Nominet has over the years supported and facilitated MPs and Peers wishing to participate in the multi-stakeholder internet governance process, such as the annual Internet Governance Forum. The company also acts as secretariat for the UK Internet Governance Forum which is a collaborative partnership that provides a forum in the UK to engage industry, government, parliament, academia and civil society in debate on issues facing the internet. We welcome any parties who wish to participate in the activities of the forum.

11 May 2018

Emma Nottingham, University of Winchester; Marion Oswald, University of Winchester; and Helen Ryan, University of Winchester – written evidence (IRN0018)

Written evidence submitted by:

Marion Oswald (corresponding author)
Senior Fellow in Law and Director of the Centre for Information Rights
University of Winchester

Helen Ryan
Senior Lecturer in Law,
University of Winchester

Emma Nottingham
Senior Lecturer in Law,
University of Winchester

Introduction

1. This submission is concerned mainly with the first two questions posed by the inquiry, namely the need for specific regulation for the internet, and the liability of online platforms. It also touches upon questions five and six regarding online safety and use of personal data.

2. This submission focuses only upon the depiction of young children on digital, broadcast and online media, and connected to this, concerns around the misuse of the digital person (the misuse of digital information/information online that represents the fundamentals of a person).

The legislative, regulatory and ethical framework surrounding the depiction of young children on digital, online and broadcast media

3. Widespread concerns around the privacy impact of online technologies have corresponded with the rise of fly-on-the-wall television documentaries and public-by-default social media forums allowing parallel commentary, with hashtags positively inviting such commentary. Although information about young children has traditionally been regarded by society, law and regulation as deserving of particular protection, popular documentaries such as Channel 4's 'The Secret Life of 4, 5 and 6 year olds' raise questions as to whether such protections are being deliberately or inadvertently eroded in the digital age.

4. Our research into this particular documentary series highlighted the risk of abusive and potentially revealing social media activity associated with the programmes. It also highlighted the contrast between the ethical and regulatory regime surrounding the use of young children in 'experimentation' in the offline world, and that which appears to be in place for the use of young children in 'Science Entertainment' and their subsequent depiction on digital media and the wider internet. The involvement of academics and health professionals gives credibility to the badge of 'Science Entertainment', yet our research indicated that institutional ethical approval processes had not been untaken in relation to these activities. We recommend that the ethical review process within academic and medical bodies be strengthened to ensure that no research-related activity of staff involving children, especially that which encourages parallel online activity impacting a child's privacy, falls outside the process.

5. There appear to be significant issues with both the relevant law and oversight processes relating to images of and information about young children on broadcast and social media. Neither data protection law nor the tort of misuse of private information seem to deal with the fundamental question of whether the children *should* have been so exposed, instead relying to a large extent on the consent of parents (which may not be objective if gain is involved). Although, in theory, a child when older could exercise her 'right-to-be-forgotten', the practicalities of doing this in respect of a volume provider such as Twitter should not be underestimated.

6. We believe that the legal and ethical framework has failed to keep track with the changing nature of broadcast programming; it is now less ephemeral, often available for long after original broadcast on the internet via on-demand services or repeated on various spin-off channels, with social media interaction making that broadcast part of the online record, and digital technologies and search tools giving access to information that an individual might have assumed was out of reach or hard to find.

Misuse of the digital person

7. We suggest that more public conversation is needed around the apparent digital social norm that accepts the objectification of young children, the posting of negative comments and images where it might reasonably be expected that the child would not agree, yet requires a best interests test to be applied in offline settings such as health and education. We recommend further consideration of how we want our young children to be treated in the offline world so that the digital world can be held to the same standards, and the inclusion of compulsory ethics processes.

8. We are concerned with the lack of protection for children in 'YouTube families' and other instances where checks on material in the public domain are either non-existent or limited, yet videos and images of young children, often in a home or

family setting, are being exploited for gain (by the social media provider, the parents and/or the agents). This contrasts starkly with the regulation provided for child actors and performers.

9. We recommend the appointment of a 'Children's Commissioner for Media, Broadcast and the Internet' to ensure that the interests of children who lack the capacity to consent to participation (in all forms of digital publication) are independently and impartially represented and protected.

10. We argue that it is no longer satisfactory that online intermediaries continue to benefit from unqualified 'mere conduit' and 'hosting' protections in EU and UK law when it comes to activities on those platforms that may be harmful to young children's privacy and best interests. We suggest that online intermediaries should have a duty of care to consider young children's privacy and best interests in their operations.

11. As part of the above-mentioned duty of care, the settings on social media services (e.g. Facebook and Twitter) should be privacy respecting as default when images or information about young children are concerned. Potentially, it should be possible to require that warnings be shown where social media systems detect that a person intends to post images of young children without these privacy settings enabled. The duty of care should increase in line with the extent to which the social media service promotes, controls and profits from the publication of images or videos of young children, for instance in the case of YouTube families.

12. There should be a limitation on the extent to which information and images relating to a young child can be copied, re-contextualised and re-shown in a different context to the original post or publication. This includes copying or sharing posts and images from social media or clips of televised programmes being shared on the internet, subsequent to its broadcast. There are new developments, such as image-matching, tracking and content moderation technologies, which could be beneficial to protect a young child's privacy and could be deployed by online services to prevent the re-contextualising of images and information (as has already been done in relation to sexual abuse images and terrorist related content).

13. It is not our intention, however, to argue that young children should not appear on broadcast or digital media because of the risk of potential harm. We agree that media of all kinds should continue to reflect the lives of children, and that parents and other adults have freedom of expression rights of their own that should be respected. We recommend that consideration is given however to new models that recognise the challenges of protecting privacy in an age when much information is exposed online as a matter of course. The misuse of the digital person model referenced below (Oswald, 'Jordan's dilemma' 2017) considers what might be the most personal or 'private' of information or activities, even if these are exposed online or digitally, and how an individual might be protected from inappropriate intrusion based on the exploitation of this information. It does not attempt to hide information already in the public domain. In this model, discernible

digital information that falls within the fundamentals of a person (for instance, an anonymous image) can be viewed, read, searched, stored, linked to and reported upon, but not further used (unless an exception applied) to generate new information or intelligence about an individual that falls within the fundamentals of a person. It may be that stricter standards regarding intrusion into a child's 'digital person' could be contemplated.

14. We note the introduction of clause 123 into the Data Protection Bill which requires the Information Commissioner to prepare a code of practice which contains such guidance as the Commissioner considers appropriate on standards of age-appropriate design of relevant information society services which are likely to be accessed by children, and in doing so the Commissioner must have regard to the best interests of children (clause 123(7)). We suggest that this code creates an opportunity for standards to be set – not only for services that are accessed by children – but for services on which young children are featured (whether or not with their consent), again having regard to the best interests of children.

15. Further detail can be found in the following open access publications:
Marion Oswald, Helen James [Ryan] and Emma Nottingham (2016) 'The not-so-secret life of five-year-olds: legal and ethical issues relating to disclosure of information and the depiction of children on broadcast and social media' Journal of Media Law 8(2)
http://www.tandfonline.com/doi/full/10.1080/17577632.2016.1239942?src=recsys

Oswald et al., 'Have 'Generation Tagged' Lost Their Privacy? A report on the consultation workshop to discuss the legislative, regulatory and ethical framework surrounding the depiction of young children on digital, online and broadcast media' 9 August 2017 http://repository.winchester.ac.uk/826/
Marion Oswald (2017) 'Jordan's dilemma: Can large parties still be intimate? Redefining public, private and the misuse of the digital person' Information & Communications Technology Law 26(1)

http://www.tandfonline.com/doi/abs/10.1080/13600834.2017.1269870

10 May 2018

Tony Stower, Head of Child Safety Online, NSPCC and Professor Sonia Livingstone – oral evidence (QQ 71-82)

Transcript to be found under Professor Sonia Livingstone

Oath – written evidence (IRN0107)

About Oath

Oath is a house of technology and media brands, established in June 2017 and bringing together familiar names including Huff Post, TechCrunch, Makers, Tumblr, Yahoo News, Build and Ryot.

Oath occupies a unique space in the UK's digital media landscape. We are a digital-only business spanning journalism and news publishing, original content creation, and aggregation of licensed third-party news and lifestyle content. We distribute our own content both on our branded sites and via commercial partnerships and third-party platforms. Through our advertising solutions, we monetise our content and partner with publishers to help them monetise their content. We also operate hosted user content and search services. We are simultaneously a creator, news publisher, rightsholder, platform, aggregator, navigation tool, online intermediary and licensee.

Our business represents a snapshot of today's media landscape – a complex, dynamic, innovative and fast-moving ecosystem.

Oath is a values-driven business. Our values are the touchstones for how we create, code, build brands, give back and lead the future. As we unify our business under the Oath brand, we apply our values to define thoughtful positions and responsible action on the key issues of the day. For example:

- Oath has joined the Internet Watch Foundation, and is building on Yahoo's participation in the IWF's hash-sharing pilot;

- Oath has taken on Yahoo's leadership position in the Global Network Initiative and Oath published its first transparency report in December;

- Oath formally launched its Business and Human Rights Program in January. This builds on a decade of Yahoo's prior program initiatives in this area;

- Oath has fostered a closer partnership with the Global Internet Forum to Counter Terrorism and has joined the industry hash sharing consortium;

- Oath was the proud sponsor of the Safer Internet Day education packs and our brands raised awareness of the event through a pro-bono advertising campaign and media coverage in both Yahoo News and Huff Post UK.

Responses to call for evidence

1. ***Is there a need to introduce specific regulation for the internet? Is it desirable or possible?***

Oath – written evidence (IRN0107)

1.1 It is important that this inquiry establishes a clear definition of what the internet is and is not.

1.2 We would encourage the committee to consider 'the internet' a technology and an enabler of business models, rather than a stand-alone thing that lends itself to regulation. It is the markets and activities which are connected to, and rely on, the internet which should be the committee's main focus.

1.3 Many of these markets and activities are regulated already, in spite of the portrayal of the internet as being the 'wild west'. The body of existing law applies online as it does offline, albeit with the additional challenges of jurisdiction arising from the global character of the internet and the cross-border reach of digital services. Thus, there is no absence of law. Rather, issues arise around how and what law applies to the digital environment, how laws are enforced online and the extent to which law might need to adapt to the digital environment.

1.4 More generally, the committee's question taps in to a lively and topical debate about what are the most appropriate legal and policy responses to the challenges arising online, particularly in the field of user conduct and content. There is an understandable clamour for answers to these novel and complex issues. Paired with an expectation of quick answers, this is the most difficult environment in which to develop considered public policy for decades.

1.5 We note that some respondents and witnesses have expressed anxiety that this environment could yield hastily crafted policy or regulation which may miss its target or have unintended consequences. While there is agreement on the desirability of finding solutions to complex problems, and a belief that effective solutions are possible, they may not be achieved in the traditional way. In these respects, it matters greatly *how* policy is developed in the digital space.

1.6 Given what is at stake for the long term health of the digital economy, there is a need to reach beyond generalities and drive policy conversations towards a detailed focus on the specific problems to be solved for. During the 90s and early 2000s, the UK enjoyed a strong reputation for thoughtful and consultative processes based on established evidence which were instrumental in the UK establishing itself as a thought leader on internet policy and building confidence in the UK as a place to invest. UK government impact assessments, for example, have been influential in how EU legislation has developed. These approaches remain a crucial foundation to policy-making but there has been a tendency to skip these steps, which coincided with the down-sizing of central government departments.

1.7 The committee should be sceptical of comparisons between the internet and its analogue antecedents, telecoms and broadcasting. The internet is a non-linear and complex ecosystem comprising myriad entities innovating, collaborating and contracting together to deliver and support a wide range of digital activities. Governance and control are far more dispersed in the online ecosystem, and the scale of the internet is of an order of magnitude unlike any other. These realities place unique pressures on the policy-making process, and generally do not lend themselves well to approaches or structures that have succeeded in the telecoms and broadcasting space.

1.8 It is therefore important that the policy-making process takes a fresh approach and consciously adapts to the diversity of the digital sector and acknowledges that there may be multiple ways to meet the same policy goal. This is reflected in individual company approaches, as well as joint company action and formalised self-regulatory structures. International collaboration is also increasingly yielding positive results in tackling the challenges of the day, for example through the GIFCT. The UK's support for such initiatives has contributed to their effectiveness and there should continue to be a space for this in the UK's policy response.

1.9 A striking feature of today's policy debate is how it is almost wholly driven by the urgent issues of the day as they are experienced on a small number of online services, typically market-leading social media platforms. This results in a policy-making process which does not fully reflect the diversity noted above and can unfairly homogenise the industry. This tends towards uniform approaches on a small number of issues regardless of whether all companies experience the same issues, whether alternative approaches would be more appropriate or proportionate, and whether companies have different issues which require their attention and resources. Tolerance for a more flexible and 'mixed' approach is therefore key, as is an appreciation that novel approaches can take time and effort to establish and refine.

1.10 The government has set twin goals of making the UK both a safe place to be online and the best place to do digital business. Care needs to be taken to ensure that the policy-making process does not put these goals in tension. The drive for uniform policy interventions have the potential to impose disproportionate burdens on companies many orders of magnitude smaller than the market leaders. If formalised in regulation or law, they can serve as regulated barriers to market entry and impact companies' ability to compete effectively. We ask that the committee is mindful of this and encourage flexibility and proportionality as to how to achieve policy outcomes.

1.11 Where there are common issues, experience shows that over the longer term, the most impactful approaches stem from broad collaboration across the industry – the 'varied ecology' model noted above - with companies adopting different practices according to the nature of their business and at different speeds, from new companies at early stages of adoption to market leaders developing and testing cutting edge technologies or partnerships with relevant public authorities. The work of the Internet Watch Foundation is a good example.

1.12 Constructive engagement between government and companies is key and some good structures are in place. However, some of the fastest growing services used by UK consumers are based in new locations such as Russia and China and government needs to develop a strategy to engage these companies and secure their commitment to the policy discussions and initiatives that are relevant to their services. These companies need a very different approach, without impeding or punishing coalitions of engaged companies. This approach has worked well in the field of counterfeiting for example. Authorities, including the UKIPO, have had a separate programme of engaging e-commerce platforms in China, while other companies have partnered on self-regulatory schemes - such as the EU MoU on counterfeiting - to tackle trade on counterfeit goods.

2. What should the legal liability of online platforms be for the content that they host?

2.1 The current scheme for attributing liability for illegal content online stems from the EU's eCommerce Directive, Articles 12-15. This is an area of intense debate although often misunderstood and we expect the committee will hear a variety of accounts of how - and how well - the current framework functions.

2.2 Contrary to the view that the framework is 'superannuated' and is losing its relevant in today's online environment, legislators at the time made the framework deliberately forward-looking and prescient by design. It was recognised from the outset that the internet was different and that, as noted above, it is a non-linear complex ecosystem comprising myriad entities innovating, collaborating and contracting together to develop and support a wide range of digital activities.

2.3 From the perspective of an online intermediary, the current framework has a number of key strengths:

2.3.1 The underlying principles have stood up well to the evolution of technology and services. In particular, their application to specific activities not business model or technology has allowed them to adapt to complex and fast-evolving business models. For example, the principles can be applied to different activities undertaken by the same entity such as an online newspaper which has limited liability for hosting user comments but full liability for its own editorial content. The principles have proven adaptable to new online activities not known at the time the Directive was drafted.

2.3.2 The principles are broadly similar to liability schemes in the offline world thus ensuring consistency between offline and online i.e.: strict liability on the originator and fault or knowledge-dependent liability on a distributor. The same approach is reflected in laws on copyright, product liability and financial services for example.

2.3.3 Although the scheme focuses on the role and responsibilities of online intermediaries, it provides for and safeguards the broader interests of third parties such as freedom of expression and of the press, as well as creative and political freedoms. In the years since the ECD was enacted, the principles underlying this balance have repeatedly been recognised in case law.

2.4 Shifting liability for online offences to intermediaries is laden with practical consequences for the ecosystem at large. Removing a long-standing common law principle would undermine government's goal of having the law apply the same online as offline, and disincentivise business transition to digital as a result. If replaced by a technology-specific or business model-specific drafting, attempts to distinguish satisfactorily between different contexts would inevitably leave unintended gaps and overlaps. Uncertainty as to how future (as yet unknown) offerings would fit into specific models brings the associated risk of chilling innovation and inhibiting future developments. Intermediaries - such as domain name registrars, hosting providers or security service providers - would become litigation targets by those seeking to enforce third party rights or by malicious actors seeking to disrupt parties relying on a particular intermediary activity. This would compromise the ability of businesses to control their online distribution chains. In short, change would unsettle a delicately balanced ecosystem built on the certainties of the current scheme and introduce risks that cannot be readily managed via contract.

2.5 The real challenge behind the committee's question is what action responsible platforms can and should take to address illegal content and conduct and how that provides clear and equitable outcomes for the parties involved. Shifting liability between parties does not provide an answer to this question.

2.6 There is unlikely to be a single action or intervention able to provide a quick fix. Online content and conduct can span the full spectrum of civil and criminal offences and often engages the rights and liabilities of parties other than the intermediary and the user. It will therefore be necessary to consider the detail of specific areas of law and understand the offences and rights to be solved for, in order to develop actionable responses which deliver the outcome that parliament seeks.

2.7 Formalised notice and take down processes are helpful in addressing some kinds of content. For example, the process set out in the US Digital Millennium Copyright Act (DMCA) s512 assigns roles and responsibilities among the relevant players – the user, intermediary and rightsholder – with each being accountable for their claims and conduct. They also address testing questions such as what constitutes a legally valid notice and actual knowledge, as well as whether any limitations and exceptions apply. The UK parliament sponsored a similar scheme in the Defamation Act 2013 which defines the responsibilities of intermediaries, allows users to take legal responsibility for the content they post and provides for victims to engage directly with the user to defend their reputation.

2.8 There should also be some focus on the treatment of content and conduct in complex cases, particularly where they touch on speech rights. Today's policy debate has come to expect intermediaries of all kinds – including domain name registrars, providers of security platforms and B2B marketplaces – to be omniscient and develop processes to ably adjudicate third party disputes which span the full spectrum of civil and criminal law (often across multiple jurisdictions, in addition to their governing law). In the offline environment, courts and other competent authorities would be expected to have some role in resolving such cases. We would invite the committee to recognise the need to define a role for competent authorities in this regard.

2.9 The vast majority of intermediaries act in good faith and want to take responsible and proportionate steps to create a positive environment for their users. The concept of a Good Samaritan defence for such action merits exploring. This performs an important role in the US Communications Decency Act by providing a defence for good faith actions aimed at safeguarding online communities through content moderation.

2.10 There is a place in the policy conversation to explore how technology can help address platform abuse and safeguard vulnerable users from harms. While technology can help identify certain types of suspect content, it does not provide a determination of legality in different contexts. It remains the case that technology and machine learning are still early in their evolution and human review, particularly for subjective content like hate speech, remains essential.

2.11 We welcome Government's support for the development of new technologies. We encourage flexibility in the levels of uniformity that can reasonably be expected in such a fast-moving market and between very diverse services. Companies may rely more or less on technology compared to peers, as a matter of policy or because of the nature of the services they provide, and certain technology solutions may be more suitable for some platforms than others.

2.12 We note above that the largest companies with the most experience of a specific issue and access to most insights about relevant content and conduct tend to lead the development of breakthrough technology which could have wider application across the digital ecosystem. This benefits the industry at large and should be encouraged.

2.13 Such technologies evolve according to a familiar pattern and are largely industry-led processes, evolving out of trusted dialogues among peer companies. For example, PhotoDNA was developed by Microsoft in partnership with Dartmouth College, and then refined and made available to other platforms via a partnership with the Technology Coalition and NCMEC. Google developed CSAI Match to detect known videos of child sexual abuse and Yahoo – an Oath brand - became the first industry partner to pilot the technology. Hash sharing to identify known terrorist-related content is also under development within an industry consortium and membership is steadily growing. We expect this type of collaboration to continue in selected areas.

2.14 We would also note that companies of all sizes can contribute to this effort and policy should value individual company initiatives which seek to solve for platform-specific issues alongside the development of high profile breakthrough technologies by the largest market players.

2.15 Finally, we note that the current policy debate can stray in to harmful content (that is not illegal but may be inappropriate for vulnerable audiences, such as children) as well as illegal content. It is important that government policy recognises that they require different responses and to provide an appropriate separation between the two in policy discourse.

3. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

3.1 We welcome the committee's attention on this question, and the potential for tension between actions intended to make the internet safer for users and the safeguarding of fundamental freedoms that individuals and businesses enjoy and are protected in law.

3.2 We have alluded above to the risk that online content and conduct becomes subject to greater restrictions than offline, and that remedies and defences individuals would otherwise expect to enjoy may be over-ridden to protect the rights of other parties or in the pursuit of well-intended public policy goals.

3.3 These are complexities which the internet industry has been tackling through a range of fora and we would encourage the committee to acknowledge their work and the important dialogue they foster, both in Europe and internationally. These initiatives provide a framework for companies to develop policies and processes to address complex issues around enforcement of law and fundamental rights and freedoms, as well as a multi-stakeholder forum to share good practice and establish accountability mechanisms.

3.4 Among the initiatives of note are the Global Network Initiative (GNI) and the Global Internet Forum to Counter Terrorism (GIFCT). 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 on Freedom of Expression and Privacy and Implementation Guidelines[1005]. The GNI has developed an assessment framework and members commit to an independent assessment of their efforts to implement the GNI Principles. The GIFCT is a multi-stakeholder forum focused on appropriate responses to terrorist content online and allows other companies to benefit from the work that has been undertaken by the companies that are seen as the primary targets for the upload of such content.

3.5 We would encourage the committee to value and support this work and encourage time and space in the UK policy discussion to engage in the important issues they raise. UK government's continued engagement in them remains important.

3.6 We have also noted above the trend in expecting companies – via individual company action or industry self-regulation - to adjudicate complex cases involving speech rights and other complex legal frameworks. This is a notable expansion on the traditional understanding of 'self-regulation' and is worthy of further examination. It is important that the committee acknowledge that it remains important that the courts should step in to adjudicate on complex cases and develop case law which can inform future policy and practice.

4. What information should online platforms provide to users about the use of their personal data?

4.1 The GDPR has asked a lot of both individuals and businesses in a relatively short period of time. The GDPR places a general obligation on data controllers to be transparent about what personal data is collected and processed, as well as for which purposes. This is the most comprehensive law on transparency in the world today.

4.2 Importantly, the intention behind it – to inform and empower individuals – is an enduring one. The transparency obligations have resulted in innovative and creative approaches to communicate to users very technical information about how personal data is collected and used, and provide users tools to control how their data is used in a variety of contexts. Like other companies, Oath has developed a privacy dashboard to inform users how their personal data is processed and how to exercise choice.

4.3 It feels very premature to opine on the success of the GDPR. We would encourage the committee not to view this moment in time as an end point, rather a milestone in a longer process of transformation in how businesses engage with users to demonstrate how they process user data, the value processing brings to individual users and how they can exercise choice.

[1005] See http://globalnetworkinitiative.org/implementationguidelines/index.php

5. *In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?*

5.1 Transparency is an important way for businesses to build trust with their users. We appreciate the interest in understanding more about the approaches companies take to moderate online conduct and content or engage with government actors when it touches on users' rights and freedoms.

5.2 Companies, including Oath, continue to develop voluntary programmes around transparency. These focused initially on government requests for user data (e.g.: under the auspices of the Global Network Initiative) but could develop further. We would welcome the committee's support for these voluntary efforts noting that work in this area is still evolving and maturing. These are not trivial undertakings and involve considerable investment and technical development, often over long periods of time.

5.3 We note the increasing debate about whether companies should be compelled by regulation to publish data about particular business practices, such as user reporting mechanisms. Proposals are typically based on the capabilities of the market leaders but would require other platforms to retool their user reporting mechanisms. This would divert resources away other activities, such as their own initiatives designed to safeguard their users or legitimate business investments. While well-intentioned, the committee should be mindful that prescriptive approaches could have paradoxical outcomes.

5.4 As noted in section 1, we ask that the committee support a 'varied ecology' of solutions to achieve a particular outcome. It is also important that new policy builds on existing good practice and established coalitions of engaged companies but avoids sudden changes of policy direction which can have a disproportionate impact on those who are less resilient.

6. *What is the impact of the dominance of a small number of online platforms in certain online markets?*

6.1 There is a wide-ranging and lively debate about the impact a small number of very large players has on the future evolution of the digital economy. Opinions are strongly-held and diverse.

6.2 As a 'challenger brand' to the market leaders, Oath experiences competitive pressures arising from the current market structure. However, we are also mindful that the current discussion can lack focus and specificity, and often conflates competition and non-competition issues. A policy discussion that continues on this trajectory risks maligning digital business models per se when the greater need is to ensure regulators have a clear understanding of complex and dynamic markets and ecosystems in order to direct robust economic analysis and craft policy that addresses actual competitive problems without unintentionally hindering competition. The term platform, for example, is extremely broad and needs to be more narrowly defined to consider the differences between platforms. Similarly, robust economic analysis is benefited by specific definition of markets, and articulation of specific concerns to assess.

6.3 The committee has already made a number of recommendations in this area in its inquiry "UK Advertising in a Digital Age", including a market study of digital advertising. In order to focus effort, we would suggest that the committee also recommend more in-depth economic study to identify the specific markets of concern and direct future work in this area. Ensuring competition authorities have the resources to build expertise and understanding of multi-sided platform markets with network effects and have the freedom to act are crucial to the efficient and effective functioning of competition law.

6.4 On a related issue, we observe that the growing frustration with lengthy competition law processes is in part driving a more interventionist approach to internet-related policy as an alternative way to change the behaviour of market leaders. The committee has heard evidence from many who share this view. This approach has many pitfalls including endorsing greater restrictions of online activities than offline. Deep market interventions or sudden changes in government policy generally favour incumbents and tend to bear disproportionately on other, less resilient competitors. It would be paradoxical if such interventions were to stifle the very competition that government policy aims to foster.

7. What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

7.1 The UK is planning its exit from the EU at a time when future EU policy and law relating to the internet is in a state of flux and subject to rapid and unpredictable change. The UK will lose its seat at the table and with it direct influence on future policy. This presents the UK with the twin risk of leaving like-minded EU member states without a crucial large ally and the risk that EU policy turns in a direction that may harm UK interests. New ways of influencing from the outside will clearly need to be found.

7.2 As noted above, the UK has enjoyed significant influence over the focus and direction of EU policy over the last 20 years. This has been achieved by a policy-making framework that draws on expert advice, has a robust evidence base and progressive thought leadership. How the machinery of government develops and advocates policy in a post-Brexit world will need some attention.

7.3 In the short term, the most crucial element of policy is to secure a stable and predictable legal framework for data flows between the UK and the EU, via the GDPR's adequacy process or a similar agreement with the EU. The committee has already explored this and urged government to make data adequacy a priority in the negotiations. Government has confirmed that it is. We welcome the committee’s continued attention on this issue.

June 2018

Dr Rachel O'Connell[1006] – written evidence (IRN0075)

1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

There is a growing recognition amongst a range of stakeholders of the need to move beyond a self-regulatory approach to a co-regulatory approach- on social media platforms in particular. Specifically speaking, regulatory oversight would ensure greater transparency, accountability and Quality Assurance concerning the handling of reports submitted by internet users about content, contact, conduct and commerce-related abuse, which is both desirable and possible. Consumers benefit when there is recourse to a regulator, and regulatory oversight results in raised standards and a cycle of continual improvement.

Section 52 of the Communications Act 2003 places a duty on Ofcom to set general conditions to ensure that communications providers establish and maintain procedures to, amongst other things, handle complaints and resolve disputes between them and their domestic and small business customers.

General Condition 14 (GC14) is the relevant condition for complaint handling and dispute resolution. Auditing how mobile operators handle customer complaints falls under Ofcom's remit. For example, in a recent investigation conducted by Ofcom, it was found that Vodafone failed to comply with Ofcom's rules on handling customer complaints. Ofcom reported that Vodafone's customer service agents were not given sufficiently clear guidance on what constituted a complaint, while its processes were insufficient to ensure that all complaints were appropriately escalated or dealt with in a fair and timely manner. Vodafone's procedures also failed to ensure that customers were told, in writing, of their right to take an unresolved complaint to a third-party resolution scheme after eight weeks.

On February 12 2018, Ofcom announced that it was extending its own initiative Monitoring and Enforcement Programme regarding complaints handling. This extension will enable Ofcom 'to continue its work in this area which has delivered positive results for consumers over the last 24 months, including improvements to Communications Providers' (CPs) complaints handling processes, (including customer service areas), and increases in the volume of ADR letters being sent'.

Currently, there is no equivalent regulatory oversight of social media platforms. If for example Ofcom's role were to be extended to social media platforms so that similar powers to investigate how reports of abuse relating to UK Internet users are handled would ensure, greater transparency, accountability and better mechanisms for redress.

[1006] Founder of Trust Elevate.com, co-founder of TheTrustBridge and technical author of the PAS 1296 Age checking code of practice.

In 2014 – 2015, Ofcom chaired a multi-stakeholder group that created a guide for providers of social media and interactive services with examples of good practice from leading technology companies[1007] and advice from NGOs as well as other online child safety experts. Its purpose is to encourage businesses to think about "safety by design" to help make their platforms safer for children and young people under 18. The guide is a more detailed version of the 2009 EU Safer Social Networking Guidelines, which are mirrored in the 2010 updated UK Good practice guidance for the providers of social networking and other user-interactive services. So, in other words, consensus on these recommendations has existed for a long time and, arguably, the next phases involve assessment the development of auditable standards.

A sensible approach would be to update the existing Ofcom guide for providers of social media and interactive services and have external assessors conduct a review of how companies adhere to the recommendations with respect to handling reports, for example the following are some the key recommendations in relation to dealing with abuse.

Dealing with Abuse/Misuse

1. Tell users at sign-up, and again through reminders, what content or behaviours constitute abuse and misuse of your service.

2. Prepare abuse reporting and take-down processes that your users and team understand.

3. Make your abuse report system accessible and easy, and offer it regularly.

4. Have a clear reporting & escalation process that can respond to different types, and urgencies, of reports.

5. Work with experts to give users additional information and local support.

Dealing with Child Sexual Abuse Content and Illegal Contact

1. Give your users a standardised function for them to report child sexual abuse content and illegal sexual contact.

2. Have a specialist team, who are themselves supported, to review these reports.

3. Escalate reports of child sexual abuse content and illegal sexual contact to the appropriate channel for investigation.

4. Tell users how they can report child sexual abuse content or illegal sexual contact directly to the relevant authorities, and/or where to obtain further advice.

The Ofcom guide for providers of social media and interactive services describes desirable outcomes but not the specifics on how they should be achieved, that's up to the organisation to decide. Facebook recently published its internal Community Standards enforcement guidelines. This is a good first step, which can be followed by companies allowing external assessors access to abuse management teams. The objective of letting assessors review processes and procedures is learning; if more effective handling of reports is what we want to achieve, are we doing the right things? From a review of these assessments, it should be possible to move toward a 'standard', which is a set of clear processes and procedures detailing, for example, how staff should be trained and what handling of reports in a fair and timely manner involves, and well-defined escalation and quality assurance processes. Once standards have been developed, an external auditor's role is to check firstly whether the described process conforms to the standard and, secondly, whether the platforms are following the described process.

Ofcom is having a lot of success check mobile operators complaint handling processes, and it would be good to explore the scope to extend Ofcom's remit and to learn to social media platforms and the thorny issue of how reports of abuse are handled.

Children and young people online

According to Ofcom 50% of 3-5 year old and 90% of 8-11 year old are online. The EU General Data Protection Regulation (GDPR) which comes into force in May 2018. Article 8 states:

> Where the child is below the age of 16 years, such [data] processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

The Article 29 working group guidance states that

> Although the need to undertake reasonable efforts to verify age is not explicit in the GDPR it is implicitly required, for if a child gives consent while not old enough to provide valid consent on their own behalf, then this will render the processing of data unlawful.

One of the recommendations the global think tank, the Centre for information Policy Leadership report on GDPR Implementation In Respect of Children’s Data and Consent states:

> That a widely recognised, effective and reliable method of parental verification, which can be applied globally should be supported by regulators and developed together with industry.

The Ofcom guide for providers of social media and interactive services includes a section on minimum age limits which recommends that social media platforms:

> Be clear on minimum age limits, and discourage those who are too young.
>
> 1. stay informed about the development of a public standard for age verification by the British Standards Institute

On March 8, 2018 The British Standards Institution published the PAS 1296 Age Checking code of practice. This PAS is written to assist those businesses that are mandated to comply with legal requirements in conducting age checks. It provides recommendations on the due diligence businesses can exercise to ensure that age check services deliver the kind of solution that meet a business’s special regulatory compliance needs.

Traditionally, to verify that an individual is, for example, 18+ years of age, the collection of a significant amount of personal data, including name, address, and date of birth, is required. In effect, age verification involves a full identity verification process. Recent technology and policy innovations in the electronic identity sector mean that it is now possible for age check services to check a single attribute of an individual’s identity (i.e. age-related eligibility). For this reason the term “age checking” is used throughout the PAS to differentiate between traditional methods of age verification and those currently available on the market. Age check services can meet the needs of a range of age-rated services that might require either a specific age or the age band into which a customer fits, which might be for instance over 18, or under 13 years of age. An age check elicits a yes/no response to a query, for example, is this person over 18 years of age or is this person below 13 years of age.

Third party age check providers will need to be certified and the Age Check Certification Scheme which is a trusted independent third party certification service to the age verification industry.

How information services handle children data online falls under the remit of the ICO. The BBFC was recently appointed the UK's age verification regulator and also has a role concerning the Audio Visual Media Services Directive and age-rating content. If Ofcom’s role were extended to cover how social media platforms handle reports submitted by or about specific customers, which would include children and young people age checking would also be a focus of Ofcom's attention.

Dr Rachel O’Connell – written evidence (IRN0075)

Global platforms

A concern that is frequently raised in discussions about regulating global platforms is the current lack of and need for some level of coordination and collaboration between governments. If the goal for the UK Government, and others, is to raise the standards of consumer protection across these global platforms, it is important to recognise that this is not new ground, and that there are tried and tested approaches that have been effective in the context of data protection and financial services. These approaches involve engaging in global standards setting, participating in various task forces and work streams, contributing to expertise via policy committees, facilitating avenues of communication between supervisory authorities in other countries and cooperation and coordination between regulators, consumer bodies and think tanks. However, collaboration with other governments need not be an impediment to either extending the remit of an existing UK regulator, consolidating the roles of a number of regulators or, indeed, creating new regulators.

May 2018

Ofcom – oral evidence (QQ 128-134)

Tuesday 9 October 2018

Watch the meeting

Members present: Lord Gilbert of Panteg (Chairman); Baroness Benjamin; Baroness Bertin; Baroness Chisholm of Owlpen; Viscount Colville of Culross; Lord Goodlad; Baroness Kidron; Baroness McIntosh of Hudnall; Baroness Quin.

Evidence Session No. 15 Heard in Public Questions 128 - 134

Examination of witnesses

Kevin Bakhurst, Group Director, Content and Media Policy, Ofcom; Yih-Choung Teh, Group Director, Strategy and Research, Ofcom.

Q128 **The Chairman:** Welcome to this meeting of the House of Lords Communications Committee and to our inquiry into regulation of the internet. We have evidence today from Ofcom and the Competition and Markets Authority.

We start with witnesses from Ofcom. Gentlemen, thank you very much for joining us today. Today's session will be broadcast online and a transcript will be taken. Can I ask Mr Yih-Choung Teh and Mr Kevin Bakhurst to introduce themselves and to tell us a bit about Ofcom's remit and their roles within it? In your introductory remarks, could you tell us what the current role of Ofcom is in relation to regulating online and whether you feel that you have the necessary resources and enforcement powers to meet your remit?

Yih-Choung Teh: I am group director for strategy and research. I will start by making a couple of points by way of context. We very much appreciate the opportunity to provide evidence to you today. Previously, Ofcom provided input into your inquiry into children and the internet. We are very conscious of your valuable thinking and contribution across this whole area.

As the UK's converged communications regulator, we are aware of the growing public debate about online harms. Indeed, you will have seen from our recent research that four out of five adults have concerns about going online. As you are aware, Ofcom oversees telecoms, post, broadcast TV and radio. You will have seen our recent discussion paper concerning online harms. Our intention was not to put forward proposals, but to make a contribution to the debate. Convergence means that communications companies are increasingly in the business of telecoms content and distribution online. We very much hope that our experience and the principles we have learned from broadcast regulation can be helpful as policymakers consider any regulation that might help to address harmful content online.

Kevin Bakhurst: I echo my colleague's comments. Thank you very much for having us here today. My job is group director of content and media policy at Ofcom, so I have responsibility for broadcasting and media, as the title might suggest.

One of your questions was about our current responsibilities in this area. You will be aware that we license around 2,000 broadcasters at the moment; 300 of those are on-demand services, available online. They include Amazon Prime and services such as ITV Hub, All 4 and BBC iPlayer. Since 2016, under the charter and agreement, we have some oversight of the BBC's online activities. That is different from the way we regulate the broadcast content; we have an advisory role in relation to the online content, but we have some responsibility in that area.

You will also be aware that we have responsibility in the field of media literacy. Primarily, that involves research and liaising with experts and so on, and trying to do relevant research to inform people in the area. That is an area we are looking at currently. We feel that we may have to approach some different areas. Baroness Benjamin will be aware that, in children's content, we are doing a significant bit of research about children's habits on YouTube and so on as part of our work. We also have responsibility for media plurality, which takes into account online as well as traditional media areas. In our recent work on Fox and Sky, and on Trinity Mirror and Express Newspapers, we very much had to take into account the online area as well.

Yih-Choung Teh: We also have some broader responsibilities that include online. We ensure effective competition. We have concurrent powers with the Competition and Markets Authority, which I know you will hear from shortly, to conduct market studies and to enforce competition law. We protect consumers from unfair practices. That could be the discovery of content or the distribution of content. At the network level, we ensure that critical services and the underlying network are secure and are available to users, and we oversee net neutrality rules. We have a limited role on the privacy of electronic communications.

The Chairman: Let us stick for a while with your remit and your relationship with other regulators.

Q129 **Baroness Quin:** Partly, we have the impression that some kind of co-ordination might be needed at an overall level. Are there areas of overlap in remit between Ofcom and other regulators? Are there gaps in the system? If either of those things is true, how best can we go about tackling that? Is there a need for some kind of overall co-ordinator, with a remit to look right across the horizon?

Yih-Choung Teh: I will start with the question of working with other regulators. We work very closely with other regulators, as you might expect. We have a number of mechanisms in place to ensure effective collaboration and co-ordination.

I can give you three quick examples. We have duties with regard to broadcast advertising. We have a co-regulatory partnership with the Advertising Standards Authority, so it looks after that piece alongside its responsibilities for online advertising. That results in a simpler regulatory regime for consumers and businesses.

We have done quite a bit of work jointly with the Information Commissioner's Office on nuisance calls over the last few years, and, more recently, with the research that we have put out. With the Competition and Markets Authority, we have a memorandum of understanding in place to share information and to help us understand who should take the lead on certain cases.

Informally, we participate in a number of networks. For example, we work on best practice with other economic sector regulators through the UK Regulators Network. The CMA takes the lead on mergers, but if there are issues of technical or sector expertise, we may second someone to the case team. There are a number of different ways in which collaboration is very much key to ensuring that different regulators can bring their expertise to generate the best outcome.

Kevin Bakhurst: I can give a concrete example, and I am sure you will have a chance to talk to the CMA about this shortly. We worked very closely with the CMA on the Fox-Sky takeover, and provided editorial expertise to the CMA when it was considering the competition aspects of that. There are concrete areas where we work together.

These are relatively early days for the regulators as regards the powers that we do and do not have on the internet. Certainly, our early work in considering this highlights one of the points you have just made. There are some areas, such as competition, that we currently cover alongside the CMA. There are some areas, such as content regulation, that nobody covers. We are very conscious of that. In our early work on this and in thinking about what contribution we could make to the debate, it was one of the earliest things we looked at. It is a vast area of the internet. Some areas of the internet, such as on-demand services, are covered, and will be covered increasingly after the new AVMSD regulations come into force, but, as you rightly point out, some areas—much of the online content and social media—are simply not covered by anybody at the moment.

Baroness Quin: Do you have discussions with government about how to improve co-ordination and coverage across the piece? Are there ongoing discussions about that?

Yih-Choung Teh: There are discussions. Ultimately, institutional arrangements are a question for government and Parliament.

Part of your question was about the benefits of an overarching body. There are some real attractions to that proposition. I am conscious that regulators such as Ofcom could benefit from a facilitating body that could help us with our digital capabilities and understanding. There is some echo of that in the Doteveryone proposals from Baroness Martha Lane-Fox on regulating for responsible technology. The Government are looking at how the Centre for Data Ethics and Innovation could work with regulators. That might be a body that can help in the area of data and artificial intelligence.

Baroness Quin: Do you think that there is real urgency to this?

Yih-Choung Teh: Our research certainly demonstrates that the public are increasingly concerned about a number of different issues. As Kevin said, there are some areas, such as social media, that have little by way of specific regulation. The biggest area of concern for people that comes across in our research is protection of children—whether it is a safe environment and whether they meet online people they have never come across before. There are a number of issues.

The Chairman: Before we move on, can we look at the wider issue of co-ordination across the regulatory piece? One thing that is evident to us is that regulators face the challenge that everyone faces of keeping up with technological change and the issues that arise from it, both the risks and the solutions. Where across the piece is the responsibility for monitoring and understanding technological change and its implications for public policy and regulation? Is there a body where you all come together to do that, or would you say that it is a particular responsibility of Ofcom or one of the other regulators?

Kevin Bakhurst: It is not an easy question to answer. There are specific areas where we have responsibility. In Ofcom, we have been building up our capability in understanding the online areas we have to regulate, such as on-demand services and aspects of websites. We have been building up, and recruiting people. Recently, we recruited a new chief technology officer. We are very aware that this is an area where we have already taken on new people. We are constantly trying to make sure that we have the right skill set for the areas where we currently have responsibility.

Similarly, there are areas for which we do not have responsibility, but where we feel we want to make a contribution to the debate, as we did in our paper. We identify areas where we feel that we need more capability in the organisation. It is an evolving process. To go back to Baroness Quin's point, in the liaison with other regulators, we are very conscious, as Elizabeth Denham may have said in her evidence to you, that you may have the resource, but it is quite hard to attract the right people with the right skills to our organisations. Frankly, there are many opportunities outside, in the commercial world, that are probably better paid for people who understand data and so on. That is a particularly difficult area to recruit in at the moment.

Baroness Benjamin: I am pleased to hear that children are quite a high priority for Ofcom, which is great news. When I was at Ofcom, it always had an arm's-length policy about regulating online. Obviously, there has now been a change, because we have seen how the world has developed. You keep mentioning skills. What skills do you think you actually need in order to help you with your work and to regulate in the way the general public want you to regulate, as you said your research has shown? What skills are you looking for? Will Ofcom really take on the responsibility to be as wide and as effective as the general public want you to be?

Kevin Bakhurst: There is a wide range of skills that we need. Obviously, in my team, the content and media area, our primary focus is on broadcasting, because that is our statutory duty. Increasingly, as you will be aware from the work on children, to understand broadcasting you need to understand the wider environment. We need people with content experience. We also need people with market research intelligence in the area, who understand what questions to ask and where to get the information to inform the debate. As I have just touched on, we need people who understand data and their use; people who understand the techniques that some of the big tech companies are using, for example.

The Chairman: Those people are expensive. Can you afford them?

Yih-Choung Teh: There are some challenges, as Kevin said, in recruiting there. I do not think that means that we cannot build up our expertise. There are certain skills in data analysis and some areas of academic research that can help. There are some challenging areas, in the sense that, as we oversee the sectors and seek to keep up with what companies are doing, there is a very significant commercial aspect to how some companies operate. You want to gain some of that understanding. Some of that is more challenging when recruiting the right skill set.

Kevin Bakhurst: Baroness Benjamin, on your arm’s-length point, as the converged content and communications regulator, we felt that we had something to say in the debate about online. Obviously, we have limited duties in that area at the moment. Whatever duties any regulator, or no regulators, might get are a matter for Parliament and the Government. There is a difference at the moment. It would be a big step change if we or any other regulator were asked to recruit to take on regulatory responsibilities. There would be a big step change from where we are now in understanding. If we were asked to do the job, that would be something very different, but it is entirely a matter for government.

Baroness Chisholm of Owlpen: Are the people out there to recruit, if you want to recruit them? Are we educating people in these fields, so that it leads to their being able to be recruited to do the job, or are they just not out there anyway?

Kevin Bakhurst: There are definitely people out there. There is quite a good supply, but there is an even bigger demand. That is the problem. The demand is international. In some areas of Ofcom, quite a lot of the people we recruit are recruited internationally. We look wherever we can find the best skill set. The people are there, but you have to look hard and there is a lot of competition for them.

Baroness Bertin: Do you think that you are being creative enough in how you partner with universities? You could do apprenticeships. You could get some young people early. They may not stay with you for 10 years, but you could get them at the beginning of their careers. It could be an amazing training ground for them to go on to other things, which would make it attractive to come to Ofcom, for example.

Yih-Choung Teh: That is exactly right. We have a very successful graduate programme. For a number of years, some of the best talent we have had we have brought in as new graduates. They have then learned their trade in the organisation. As you say, we are now investing effort in looking at the apprenticeship possibilities. That is potentially a very rich vein.

Baroness McIntosh of Hudnall: Could I take you back to something you mentioned in your opening remarks about things for which you have responsibility? You mentioned media literacy. In your report, you point to that as one of the ways in which it might be possible to combat the particular harm that comes from misinformation being used to try to influence political choices of one sort or another.

First, do you see it as a growing potential source of harm? Secondly, when you say that media literacy is one of the ways in which it can be combated, how do you anticipate carrying through your responsibilities to make that better across the population?

Yih-Choung Teh: That is a very good question.

Kevin Bakhurst: Can I answer it first?

Yih-Choung Teh: By all means.

Kevin Bakhurst: This is a joint responsibility, in a way, so we can both answer the question. We have no doubt that one of the key weapons you can arm consumers with is an understanding of where they are getting their information, who is paying for it, whether it has an agenda and what their expectations about accuracy, impartiality and so on should be.

Across the world, particularly across Europe, there is an increasing focus on media literacy. This is an area for which we have had some responsibility, and we are redoubling our focus on it because of its importance in the current debate. We are now working up plans for the particular areas we should be looking at. A lot of good work has been going on elsewhere, here in Parliament and across other research bodies.

One of the questions for us is how you can better co-ordinate all the sources of media literacy. The BBC is doing a fair bit, and the *Telegraph* has been doing quite a lot on it. A lot of work has been done in Parliament, and a lot of academic work has been done. We have been talking to our colleagues at the Irish regulators, whose approach is very much about trying to bring together the best sources and making sure that they are available to audiences in the most effective way.

The Chairman: How muscular are you about that sort of co-ordination? In our inquiry some time ago into children and the internet, we found a whole range of very good work from the kinds of organisations and agencies you mentioned, and, indeed, from some of the companies in the field, but a significant lack of co-ordination. There was not much conflict between what they were doing, but there was waste and a lack of co-ordination. Is anyone taking a muscular approach to changing that?

Yih-Choung Teh: As Kevin said, it is certainly our hope to try to move forward from research to provide more of a co-ordination role. We already do a certain degree of that by participating in conferences and gathering together academics and other industry players, but I think there is more we can do.

The Chairman: You think that it is your job.

Yih-Choung Teh: I think our responsibilities on media literacy give us the potential to do that. It is something we think is very important.

The Chairman: I am trying to find out who is going to take the lead on it. Are you saying, "We are going to step up to the plate and take the lead on this one"?

Kevin Bakhurst: It is certainly our intention to step up the pace. As I mentioned, we have a statutory duty on media literacy, so we feel that we can play a leading role. I do not know whether we are the lead, but, to answer your question bluntly, there is a lot more we can do. The role of media literacy has become much more crucial, certainly for the foreseeable future.

Baroness McIntosh of Hudnall: Could you address specifically the question of the impact on the democratic process of the particular kinds of technology for which, at the moment, you do not have much responsibility, but where literacy has some impact?

Kevin Bakhurst: As we said in our paper, one of our key areas of concern is misinformation and fake news, and the impact that that has self-evidently had, and is suspected of having had, on key processes. A lot of the thinking we have been doing has been about how you can bring more transparency to the social media organisations that, frankly, are responsible for spreading a lot of information and misinformation, and how you can make sure that users know where the information is coming from. In particular, some very interesting work has been going on around Europe on elections. We are liaising very closely with our fellow European regulators about the work they are doing in France, Germany and so on about tackling misinformation.

You are quite right: a lot of this is outside our remit, because it is outside everyone's remit. That is one of the reasons why we felt we had a contribution to make. Obviously, we have experience in the area of regulating news on broadcast media, and doing so to a high standard. That is why, despite the questioning environment generally, audiences around the UK still trust news and current affairs on our regulated broadcasters very highly, as they should. The broadcasters have to live up to very strict guidelines on due impartiality and due accuracy, and audiences are clearly sophisticated enough to understand that. Part of what we were trying to do was to take lessons from the importance of PSB news, in particular, as well as commercial news on Sky and so on, to see what you could learn from that in the online space about what is valuable, what is reasonable and what principles you can start from to try to help audiences to navigate their way through the blizzard of information and misinformation.

Baroness Quin: To go back to the whole business of co-ordination, including in the areas we have just been talking about, should government designate a lead organisation? How is leadership going to be arrived at? The different organisations at the moment have their areas of responsibility, which, no doubt, take up most of their time and effort. Who should be designating a leadership role in this situation?

Kevin Bakhurst: The Secretary of State and DCMS have said that they plan to publish proposed legislation in the parliamentary winter, as you know. They are giving it careful consideration. To answer a previous question, we provide whatever information we are asked for to help their work on that. We try to make a contribution to the ongoing debate. We hope that that paper, when it is published, will give a clear sense of direction.

The Chairman: We had better move on.

Q130 **Baroness Chisholm of Owlpen:** How do you feel that Ofcom's experience in the regulation of communications can be applied to online content moderation and complaints procedures? Leading from that, Ofcom has experience of regulating broadcasting content for the internet, so what lessons do you feel can be drawn from that on the need to balance online safety and freedom of expression?

Kevin Bakhurst: Part of what we tried to address in our paper was what lessons we, as the broadcast regulator, can learn from that and what aspects of our regulation regime we feel are and are not appropriate to online. Self-evidently, broadcast is very different from online, because of the sheer volume of material and the sources. We license 2,000 broadcasters. That is a lot, but they are responsible for the material that appears on those platforms. Self-evidently, social media are not responsible. That is a conversation. They have some responsibility, but they do not generate the material themselves; it is the public. There are clearly differences.

We feel that there are some appropriate lessons that we can take. For example, we have quite a lot of experience of operating a system where Parliament has set out principles on regulation. The Communications Act was very clear on that. It sets out a requirement for a range of things. It then leaves it to an independent regulator to interpret the best way of providing those standards.

Our experience in that area could be transferable, because it allows Ofcom the flexibility to move as broadcasting moves and to adapt quite quickly as audiences change, as well as to adapt to audience expectations of the broadcasters and the different platforms, which also change over time. There could be a principles-based set of requirements from Parliament or government, and an independent body, whoever government decides that should be. We feel that gives credibility, as well as a regime, because you can be transparent, you can be based on evidence and, by and large, people will trust you to do your job and to interpret it in a reasonable and proportionate way.

I will try not to go on for too long, but there are other key areas where we feel we have experience. One is balancing the right to freedom of expression, which is really important, both in broadcast and, clearly, online, with the obligations and rights of individuals. We also have an understanding of contextual factors: what audiences expect from the BBC as regards editorial standards and so on will be different from what they might expect from a website they have never heard of.

We feel that being able to enforce effectively is really important. It is important to have a statutory base for regulation and a system where you can enforce properly, with fines or other meaningful measures, if necessary, so that people respond in the end, even if they do not want to. Those are the sorts of things that we would draw from our experience.

Baroness Chisholm of Owlpen: Somewhere in your report I think you said that you felt that one of the problems was that at the moment enforcement of online content is almost at the beginning. People are not thinking ahead to regulating before it happens, so they are not really thinking ahead about what will be designed in the future. Everything is reactive, rather than proactive. Do you think that is true?

Kevin Bakhurst: Yes, we think that is valid. I think it is in the report. Whatever the Government decide, if they decide that there needs to be some form of regulation, they should enable it to be flexible and reactive. Look at how online has changed in the last five years; no one would have predicted that. No one would have predicted the rise of Netflix and Amazon Prime in the way it has happened, or the rise of social media and their influence, or the problems with disinformation. It is happening very quickly, so, in our view, a regime needs to be based on principles. It must allow a body or regulator to respond quickly and to keep looking ahead, so that it is not regulating for yesterday's problems, but looking ahead to address today's problems.

The Chairman: Do those principles exist?

Kevin Bakhurst: Yes, there are some key principles that exist. First, it would essentially be a matter for Parliament to determine what were the key areas it wanted to deal with, whether that is protection of children, take-down of illegal content, harmful content and what Parliament means by that—bullying or whatever it may be—or misinformation. You could lay out a set of areas that need to be tackled.

Secondly, there are principles you can bring to it. One is independence of regulation, which gives a degree of flexibility and credibility, in my view. Others are freedom of expression and freedom of innovation, which are key to online. There are a number of principles that you could set as a framework.

The Chairman: Whose job is it? Is it Parliament's job to start the work on those principles and the balances between them?

Kevin Bakhurst: Ofcom exists because of Parliament, and we take our duties from Parliament. Our work on the BBC, which is quite recent, is quite a useful blueprint, in a way. Parliament set out clearly its desires for the BBC in the charter and agreement. Then it said, "We are going to appoint an independent regulator to make sure that the BBC performs to those standards". In our experience, that is a very effective way of operating. The answer is yes, it is for Parliament to set out those principles.

Baroness Kidron: Can I pick up on a couple of things? First, you said, "Obviously, they are not responsible". I am not sure that the Committee totally agrees with that. Even though it may be content that is created in some way by the public, if platforms are making money from it, curating it, privileging it or spreading it, are they obviously not responsible?

Kevin Bakhurst: Maybe I was not clear enough.

Baroness Kidron: It is a view that exists. I am not suggesting that you alone made it up.

Kevin Bakhurst: No, that would not be our view. Clearly, they have a responsibility. They are not responsible for the original creation of the content. People just do that, and they are enabled to do it until someone stops them doing it. Allowing people to do that is probably the tenor of freedom of expression, but you must have responsibility for the content that you disseminate in the end—how you do it, what you stop and what you take down.

Baroness Kidron: That is fantastic. The other thing you said that I thought was quite interesting was at the other end of the chain. You are calling for a statutory and independent look at it. I wonder whether you would like to comment on the fact that often we say that they are so powerful, and then we give them more power in the way they regulate, which ends up with people from Facebook sitting in Berlin saying, "Is this hate speech? Is this not?" Is that the sort of thing you are talking about? Do we need something that is very clear-cut for all parties about where the deciding voice is?

Kevin Bakhurst: Yes. Our view, which is built on our own experience, is that regulation works only if it has statutory backing, a clear remit from Parliament in the UK and a trusted independent body that will interpret that and set clear rules.

Germany is an interesting example, because there was quite hasty regulation ahead of an election. We looked at that quite closely, and worked closely with the German regulators. Whatever the rights and wrongs and the unforeseen consequences of what they have done there, the interesting thing about Germany is that it shows us what individual countries can do. People often say, "You can't tackle these institutions, because they are international and multinational". You can, and Germany has shown that. You can tackle them. It has forced Facebook and Google to take action in Germany.

Yih-Choung Teh: I am conscious that the platforms have started to pay more attention and to do a bit more, but self-regulation has its limitations. You made that point in your report on children and the internet; the commercial incentives mean that self-regulation will take you only so far. Kevin's point is a good one.

Viscount Colville of Culross: I want to pick up what you said about self-regulation. What role do you think the regulator has in looking at the appeal processes of the social media platforms, and whether they are effective, fair, transparent and timely?

Kevin Bakhurst: That is a tricky question, but a really important one. We have spent a lot of time looking at it. We feel there are some lessons for us from how the "BBC First" complaints system works, which is quite interesting. Viscount Colville, you will remember from the BBC that a lot of complaints come in. The BBC deals with 250,000 complaints a year. People have to complain to the BBC first, before they can come to Ofcom. We can step in if we want to, but normally it goes through the BBC first.

In our first year regulating the BBC, we ended up looking at fewer than 200 complaints. There is a substantial number of complaints, but, by and large, people go through the BBC process and get some satisfaction from that. There is a system. If you have to complain to the media organisation first, hopefully, it becomes more manageable. When it comes to online, the number of complaints is in a different sphere. The answer may be a lot more transparency about how they handle complaints and what the outcomes are. An appeals process could be extremely labour intensive for some of the big companies, so, in my view, it is not clear-cut what the best solution would be.

Q131 **Lord Goodlad:** My question is about duty of care and the legal obligation. Could you tell us what thought you have given to legislation to introduce a duty of care to prevent online harm?

Kevin Bakhurst: We were very interested in Will Perrin's and Lorna Woods's suggestions about a duty of care. In fact, we were at a very interesting and useful session organised by the Carnegie Endowment. It kicked off with their suggestions, and there was a wide-ranging discussion afterwards, which was very useful.

I have said this before, so I hope I do not get boring. To come to your point, we said in our paper that a form of principles, whether that is a duty of care or some principles set out by Parliament, is quite a good place to start. Will Perrin talks a lot about the HSE and the duty of care it has set out, but the HSE is a very big organisation to police that. The issue is whether that would truly translate, or whether just a system of principles might translate, but we think it is a really interesting idea. We have engaged with them quite closely on it. We are looking at it and having a discussion about how it might or might not work practically.

Lord Goodlad: The common law on this is very well established. It does not really extend to what we are talking about here and has to be done by Parliament in a pretty precise way. It cannot just be left to the courts, can it?

Yih-Choung Teh: The appeals mechanism that would sit on the back of it is an interesting question that would need to be considered. The question it raises is that, if the recourse that every individual has is to go through the courts, is that necessarily the best answer to some of the questions? It goes back to the question of what specific harms we are seeking to deal with. Some precision is probably required around that.

Baroness Bertin: The NCA has suggested kitemarking some websites that are aimed at children. I want to know very briefly what you think about that.

Yih-Choung Teh: There are some attractions to trying to communicate clearly with the public what are and are not safe areas. As Kevin observed, one of the advantages for public service broadcasters is that they have a brand and an identity; consumers have a certain expectation and there is a degree of trustworthiness. There are similar ideas that might be fruitful.

Q132 **Baroness Kidron:** One thing that keeps coming up for us is the scale and breadth of harms. One of the big movements now is "ethical by design"—"Let's go upstream and fix things before they happen, so that we are not constantly picking up the pieces". I would like you to say something about your thinking on that. In particular, as well as the harms we have already discussed, I want to put on the table Tristan Harris's point about addiction by design as a possible harm that we might define. I am interested to know what you have been doing around that.

Yih-Choung Teh: I will have a go at saying something broadly, and Kevin may pick up specific examples. My understanding of "ethical by design" is that it refers to applying in the design phase principles such as empathy for users, providing enough information for users to make informed choices and understanding the differing needs, abilities, viewpoints and morals of users. As an approach, it has to be very attractive so that you prevent some of the harms we are talking about by design, rather than trying to look for a cure after the event. As a parent of young children, you desperately want an online environment where you feel that they are safe by design, rather than one where you are always watching out for something.

To echo some of what we have been speaking about, for me, it probably relies on trying to identify the principles you want taken into account in the design phase. I am very conscious that this is an area of rapid innovation, where we want new services to come forward and everyone to benefit from them. You want to be conscious of not being overly prescriptive in platform standards, which might constrain some of that, but, at the same time, you want to embrace some of those principles. You would hope that those would be embedded and would generate positive behaviours and outcomes right at the outset.

Turning to some specifics, we are conscious of the age-appropriate design code.

Kevin Bakhurst: We have been following your amendment very closely. We have been working very closely with the ICO on aspects of that. I know that it is out to consultation at the moment, and following it through will probably be a substantial piece of work, both for you and for the ICO. I am sure that it could be a really useful tool in the armoury.

Obviously, it does not answer all questions, because there are huge, influential companies already distributing content to children. There are also big tech companies distributing content that children access but that is not aimed at kids alone, so it can be only one part of it. From what we have seen so far in some of the work that has been done, it is a hugely encouraging start to tackling one of the harms that, as we say in our joint research with ICO, consumers and audiences put highest: harm to children.

Baroness Kidron: The second part of this question is around enforcement. If it is only a principle, how do you enforce it? If it is a standard, maybe we can. That is the battleground. I am very interested to know about that.

Kevin Bakhurst: That would possibly come back to what I touched on earlier. You could set principles and then allow a body—ICO, another regulator or whoever the Government decide should have the responsibility—to decide practically how those principles translate into real action. Websites would have to build in certain aspects at design, if they were aimed at kids, and would then have to demonstrate transparently that they had done that to an independent body that could hold them to account for it. Platforms would have a duty to take down content that is harmful to children within a certain timeframe or to prevent it going up. They might have their community guidelines saying that they do that, but at the moment there is very little transparency about whether they are delivering what they promise to deliver. You can work from principles, and have a body that takes those principles and turns them into practical reality.

Baroness Kidron: I absolutely understand what you are saying and really appreciate it, but, for the record, what we are saying is that having principles is not ducking the issue. Principles can be met by statutory enforcement, with an independent regulator.

Yih-Choung Teh: Indeed—even if the companies themselves are putting forward how they interpret certain aspects of a code. They may say clearly themselves, "This is the information that we are gathering from children. This is how we are collecting it. This is what we are using it for. This is how parents and children can maintain some control". If that is transparent and made clear, we have the opportunity to have a body that can hold them to account.

Kevin Bakhurst: I come back to the earlier point about lessons from broadcasting regulation, where there are a lot of principles. We turn those into concrete rules. We have the statutory powers to write to the broadcasters or to go in to see what they are doing practically to deliver the standards required under the guidelines. You can translate principles through the right process, using statutory power and transparency to make sure that the outcome is correct.

Baroness Benjamin: With the BBFC, in films for children, a voice announces what they are going to see and the duty of care. Do you think that online providers should be doing the same thing and telling children, "This is what the policies are"? "Newsround" did a thing on whether children understand what they are signing up for. The children said that the writing is so small that they do not read it; they just go straight in. Do you think there should be something bigger telling children, "This is what you are signing up for"? They do not actually care, because a big enough point is not being made that "This is what you are doing".

Kevin Bakhurst: Our approach is that it should be absolutely clear to children and their parents what they are signing up for and what they are watching. The area of online content that we now regulate for children under AVMSD is on-demand children's content. There are clear guidelines around that. As we know, the BBFC is working on age-appropriate guidelines. It is not straightforward. One fear for me, as a parent of slightly older children, is that sometimes it can be an invitation, rather than a prevention, if you tell them they should not be watching it.

Baroness Benjamin: On the BBC, when you sign up, there is now a voice that tells you, "You have to do such-and-such and such-and-such and such-and-such". There is a voice that actually says it. Do you think that children need to have that on the things that are going to be provided for them? That is one way of alerting them to what they are signing up for.

Kevin Bakhurst: The voice is not the only way of doing it. They could be made to go through a process where they either have to prove that they are a certain age or it is clear to them what content they will be watching. Sometimes I look at things and think, "That isn't clear. It is a small line in the corner of a screen".

Baroness Benjamin: Exactly.

Yih-Choung Teh: It may be a good example of the principles base, where there may be different ways to achieve the outcome, but, as you say, there is something going wrong if the message is not getting across. In the same way, a company may put down lots of terms and conditions and you have to tick a box before you download the app to your mobile phone, but I guess that the majority of people do not read them. That is not really working.

Baroness Benjamin: Exactly.

The Chairman: Let us move on to TV-like content.

Q133 **Viscount Colville of Culross:** I would like to declare an interest, as a series producer working for Smithsonian Channel and CNN.

You have very clear parameters for the regulation of PSBs. However, it is a hotchpotch when it comes to the other parts of the VoD environment and the way people receive programmes. You have quite a good diagram that shows some of the chaos in regulation. Should there be a much more level playing field between broadcasters and other content providers, and in the way they are consumed?

Kevin Bakhurst: I would describe it as variable geometry, rather than a hotchpotch, but you are undoubtedly right; there are different standards, depending on how people receive their content. Yes, broadcasters are held to the highest standards. The thresholds or standards for them are higher. That is partly under statute, so on-demand content is regulated to a lower level.

At the moment, the protections for online content are designed particularly around terrorist content and protecting young people. Under the new AVMSD rules, if they are transposed, the protection of audiences will be increased slightly, but it will still be a variable geometry.

Our research shows that, by and large, audiences value the protection they get in broadcasting through regulation. They recognise that, to a large extent, the content they consume on the main broadcasters is highly regulated and that content they might find online has a different set of rules. Is there room for them to come closer together? I know that some of the commercial broadcasters would like to see a narrowing of the gap. We are always looking at what more we can do, and what we have the powers to do, to protect audiences, and the key areas where we need to act.

Yih-Choung Teh: On protecting audiences, in July we put out a document on prominence for public service broadcasters. As I am sure you are aware, our duties are constrained to linear electronic programme guides. We asked a question about whether there needs to be more to ensure that public service broadcasting is not just available, but is discoverable when people are watching on demand or on other devices. Of course, that is a question for Parliament, rather than for us, but it is an interesting point.

Viscount Colville of Culross: You are looking at that question yourselves right now, are you not?

Yih-Choung Teh: We have raised the question. I am just observing that we can look at the question of linear, and where on the EPG certain services can be. When it goes beyond linear, it will be a question for government.

Viscount Colville of Culross: We did try.

Yih-Choung Teh: I appreciate that.

Viscount Colville of Culross: My other question is about impartiality. I have been working at ITN. At ITN, they are extremely concerned by the fact that you say that people's expectations of impartiality for certain content are lower when it comes to online. Where does that leave the public service broadcasters when it comes to online and online consumption? Increasingly, that is where their news and current affairs is being consumed. Trying to maintain their impartiality in an environment where everything is about opinion and editorialisation is a problem, is it not?

Kevin Bakhurst: You might describe it as a problem. I would say that it is actually a great opportunity for the public service news organisations, because we know that audiences value the impartiality and accuracy they are obliged to demonstrate and that, for a vast amount of the time, they live up to.

As I said before, we have to make judgments about contextual factors, which include what audiences expect from individual services. When audiences are watching a mainstream, UK-focused news service such as the BBC, Sky or ITN, they have extremely high expectations, and rightly so, of accuracy and impartiality. When they are listening to LBC or Capital, it is the same. When audiences are watching other services, such as foreign news channels, that are licensed in the UK, either through country of origin or in the UK itself, or are consuming content online that has no obligations, mostly, on impartiality or, indeed, on accuracy, we know they have different expectations.

We always have to weigh up the range of views that people can get and the issue of media plurality. There is a place for opinionated news. If there were not, newspapers would not be in the market. There is a place for it in broadcasting as well, if it is clearly labelled and the audience knows that what it is watching is coming from a particular perspective. We are not in the business of shutting down a range of perspectives. It is really important for people to be able to get that. Key, at the heart of that, particularly in the light of concerns about disinformation, is the value that audiences put on ITN, Sky and the BBC, and the huge numbers who still go to them to get accurate, impartial and extremely high-quality news.

Q134 **Baroness McIntosh of Hudnall:** We are getting on in this discussion, and you might have thought that we were going to get all the way through to the end without anyone saying the word "Brexit".

Kevin Bakhurst: We were hoping.

Baroness McIntosh of Hudnall: Wrong. In an early part of this discussion, you mentioned your collaboration with European regulators in respect of issues to do with fake news, so-called, and misinformation. I have no doubt that there are many other ways in which you are collaborating with your European colleagues and, indeed, other international colleagues.

It has been put to us that Ofcom has been, and is, the lead regulator in Europe in these matters. Now it looks as though we are not going to be a member of the European Union for much longer. What impact do you anticipate that having on your ability to collaborate? What other impacts do you envisage it possibly having? Looking more broadly at international collaborations, can you see ways in which there might be opportunities in the future? Is there anything you want to tell us, given that we are discussing a global issue?

Yih-Choung Teh: I will try to make a start and then Kevin can add to it. Leaving the EU will clearly have implications, but the key observation is that we will continue to need to collaborate with other regulators and agencies globally, regardless of whether we are in the EU or not.

I say that for two reasons. First, a lot of the questions we have been discussing, such as our concerns about online harms and protection of children, are shared globally. It strikes me that there is a lot to be gained by sharing and pooling our research, understanding and learnings across a global community.

Secondly, for the most part, we are talking about companies that are global in nature. Greater standardisation and harmonisation are likely to help in reducing the costs of good outcomes, increasing the likelihood of compliance and reducing complexity. We very much want to continue to collaborate with bodies both inside Europe and not. As you indicated, we would like to think not only that we get the benefits of sharing understanding and best practice, but that we can be quite influential.

In the content space, there are certain bodies we participate in.

Kevin Bakhurst: In the content space, it is variable. On media regulation, there are two bodies in which we have played a very full role. One is ERGA, which is associated with the European Commission. Obviously, our role in that will change. We do not know what it will be. We will not be a full member, because you cannot be if you are not a member of the European Union. There is some discussion about our being there as observers. Switzerland and one or two other countries are there as observers. You can still be in the room and have a voice, but, obviously, you cannot have a vote.

There is another organisation called EPRA. In fact, tomorrow I am going to a two-day meeting of EPRA in Bratislava.

Baroness McIntosh of Hudnall: Can you tell us what the acronym means? I imagine that it is "European something".

Yih-Choung Teh: It is something like the European Platform for Regulators Association.

Kevin Bakhurst: Do not hold us to that.

Baroness McIntosh of Hudnall: We will check it.

Kevin Bakhurst: We will check it for you. We have a representative on EPRA's board at the moment. You are right to say that we are very influential in it. One of the reasons why I am going for two days is that we want to make sure that we remain influential in the organisations where we will have an unchanged role. It is a very good platform for liaising not just with EU regulators but with other regulators that are not in the EU.

At the same time, we have deliberately stepped up our international efforts. We liaise quite often with regulators from Australia, Canada and other parts of the world that are not in the EU. We have good bilateral relations with the Germans and the French, and we have seen the Swedish, the Irish and so on. We intend to carry that on, and they have made it clear that they are very keen for it to carry on. It is a very valuable forum for the exchange of ideas. There is no doubt that, in some bodies, we will be less influential, but we are making every effort to make sure that we maintain the maximum international involvement.

Baroness McIntosh of Hudnall: I noticed that the US was not in the list of territories you mentioned. Clearly, given the location of the homes of some of the biggest platforms, we would be interested to know how you anticipate developing relationships in that area.

Kevin Bakhurst: To be fair, we have been over to the US a couple of times. I went over myself, with two colleagues, earlier in the summer, when we were looking at whether we were going to make a contribution to the debate about online regulation. We went to visit both some of the regulatory voices there and the key tech firms. We went to Google, Facebook, Twitter and Reddit to try to get under the bonnet of what they are doing, what they say they are doing and what the reality of it is, to find out a little more about the culture of the companies, to find out what their view would be on a form of regulation, to discuss some principles of that and to see how they responded to it. We are engaging internationally in the States as well.

Baroness Bertin: Can I ask what you saw under the bonnet?

Kevin Bakhurst: How long do we have?

Baroness Bertin: You know what I mean. What is their general feeling?

Kevin Bakhurst: There are lots of different messages coming out. There are two universal messages. First, I think they agreed with something I suggested to all of them, which is that they have become so big, so powerful and so influential so quickly that their internal governance and the ways they handle themselves corporately have not kept up. There was no dispute on that. Some of them are running quite hard to try to catch up, but they are developing so quickly, and the issues are coming at them so fast and are so huge, that it is a challenge for them. Generally, they recognise that they are bigger than they can manage at the moment. I do not think I am giving away anything I should not.

The second thing is this. A year and a half ago, when we tried to have some conversations, they said, "Go away. You are regulators. We want nothing to do with you". Interestingly, this time they were very open to engaging. They took us in, and we met some very senior people to discuss what regulation could look like if a Government decided to legislate. We discussed some ideas we have, which are in our paper and which I have touched on, about how it might operate: principles-based and respecting freedom of expression and innovation—but bringing a whole load more transparency and requirements to what they do.

They were not unreceptive. They said that they look around the world and see that lots of countries are trying to regulate, or thinking about regulating, at the moment. I came away feeling that, if the Government decide to go down that road, there is a space for the UK to create a system of regulation that could be very effective in dealing with some of the worst harms and it could be a global model for how to do it. I do not look around anywhere and think there is a brilliant model. Neither do they, by the way. They do not like regulation very much generally, but they almost feel that, if the UK did something other countries could look at as a good form of regulation, it might be valuable to them in the long run in heading off some of the madder ideas. Those were the two headlines.

The Chairman: We need to draw the session to a close. I thank Mr Teh and Mr Bakhurst for their evidence. Do you wish to add anything that you think we might have asked, but did not?

Kevin Bakhurst: I would not suggest anything. You put us through our paces. Thank you very much.

The Chairman: Thank you very much for your evidence. It has been very useful. As we develop our report, we may come back to you to discuss technical issues.

Kevin Bakhurst: If we can provide any information, we will be delighted to do so.

The Chairman: That would be appreciated. Gentlemen, thank you very much for your time today.

Office of the eSafety Commissioner, Australian Government – written evidence (IRN0016)

1. Overview of the Office

1.1 The Office of the eSafety Commissioner was established in July 2015, under the *Enhancing Online Safety Act 2015* (Cth) (the Act). At the time, the Act gave the Office a remit of enhancing online safety for children and young people, directing the Commissioner to play a national leadership and coordination role to help prevent and mitigate the impacts of the most insidious forms of online abuse. In July 2017, the Office's remit was expanded to cover enhancing online safety for **all** Australians. A core function of the Office is its work with law enforcement and other partners such as INHOPE and industry to take action against:

- child abuse material, through our Online Content Scheme
- image-based abuse, through our Image-Based Abuse Portal
- serious cyberbullying material targeting an Australian child, through our Cyber Bullying Complaints Scheme.

1.2 These reporting schemes offer Australians practical help in managing the impact of these types of abuses, but their real uniqueness lies in the fact that the Office can formally direct online service providers to remove illegal and cyberbullying content from their services, and informally request the removal of image-based abuse; providing and empowering victims and survivors of online abuse to take control and help reduce feelings of re-victimisation. All of the schemes operate within a unique multi-stakeholder model, overlain by multi-faceted objectives – providing the Office with a unique perspective on the complex web that cyber abuse spins across all of societal structures, and the role that all stakeholders play in addressing and trying to combat this type of crime.

1.3 The Office also plays a key role in educating and empowering Australians to combat cyber abuse in all of its manifestations[1008]; to better manage the safety and wellbeing of Australians online; and to develop critical digital skills to ensure Australians feel inspired to explore and engage with the online world whilst also having the resilience to overcome online set-backs. All of this is achieved via our outreach programs in schools and in the community; the provision of web information; virtual classrooms; peer-led 'digital leaders' programs; lesson plans; face-to-face training; youth and parental information and expert guidance.

1.4 Our in-house research team creates an evidence base for everything that we do, and we have developed compelling and engaging sets of online resources at esafety.gov.au, such as dedicated portals for parents (iParent), for children and

[1008] Including, but not limited to, cyberbullying, harassment, stalking, hate speech, anti-social content, violent and distressing content, image-based abuse, offensive or illegal content, sexting, unwanted contact, child sexual exploitation, online grooming, and social engineering.

young people (Young and eSafe) and for women experiencing technology-facilitated abuse (eWomen). The Office also manages and supports NGOs and safety experts to deliver their own online safety programmes and presentations to schools, through our certified providers program. The Office proactively engages with the Australian media to raise awareness and understanding of all forms of cyber abuse, as well as providing the public with tangible solutions and strategies to help navigate the online world safely.

1.5 Collaboration and multi-stakeholder engagement are pillars in the Office's strategy to combat online abuse. The Office serves as the national leadership and coordinating body for online safety within Australia. It facilitates the Online Consultative Safety Working Group and the eSafety and Mental Health Working Group, both of which are comprised of online safety and mental health experts representing all sectors of the economy. The Office also engages at an international level, collaborating with key players in the wider global community in order to achieve the best outcomes for children and young people, and to assist in the development of evidence-based strategies to end violence against children in particular.

1.6 In our experience, taking a holistic approach to online safety issues has proven to be the most effective approach. Key to harm minimisation is the take down of harmful or "serious cyberbullying content" before the bullying escalates or the conduct reaches a criminal threshold. Australians, and particularly young Australians, need tangible, rapid redress – and our comprehensive powers have been proven to do just that.

2. Cyberbullying Complaints Scheme

2.1 The Office manages a world-first complaints system for serious cyberbullying of Australian children, where children, parents and teachers can lodge a complaint and receive timely advice and assistance. In its almost three years of operation, we have assisted over 760 children and families with rapid take-down of harmful material from social media services. We have played a critical role in helping address specific cyberbullying incidents, acting as a safety net to prevent harmful behaviour from escalating.

2.2 Key to our success is the cooperation shown by social media services when responding to informal requests to remove material, and our hybrid approach in targeting the root cause of the social conflict. We have had a 100% compliance rate with social media services to-date, and therefore, have not needed to exercise our formal powers to achieve take-down. The Office also works with parents, schools and when necessary, law enforcement, to get to the core of the problem as cyberbullying is often an extension of what is happening within the school gates. Early intervention through reporting, followed by collaboration with school communities and education can help address and quickly alleviate the harm that can arise from cyberbullying. In cases where a complaint identifies that cyberbullying may be a systemic problem in a particular school, the Office will deliver targeted presentations to parents and teachers to help combat the culture and provide relevant resources and tools to better protect students.

Functions of the Scheme

2.3 The Act established a two-tiered scheme for the rapid removal from social media services of cyberbullying material targeted at an Australian child. The two tiers of the scheme are subject to different levels of regulatory oversight; Tier 1[1009] social media services participate in the scheme on a co-operative basis, whereas those services that do not opt in to become a Tier 1 service or are declared by the Minister for Communications to be Tier 2 social media services are subject to legally binding notices and penalties.

Tier 1

2.4 Providers of Tier 1 social media services may elect how complaints made to the Commissioner should be assessed and notices given. This can be against either the 'default rule' set out at s.29(1) of the Act or the 'special rule' set out at s.29(2) of the Act.

2.5 Under the special rule, Tier 1 providers have the option of any assessment by the Commissioner of whether particular material is cyberbullying material being first made by reference to the social media service's own terms of use, rather than by reference to the definition of targeted cyber-bullying material in the Act. The choice between the default and the special rules is given effect by way of a statement from the social media service provider, under s.23(3) of the Act. If cyberbullying material is posted on a Tier 1 service the Commissioner can issue a notice requesting removal of the material within 48 hours. If a Tier 1 service does not comply with a written notice, under s.39 of the Act the Commissioner may draft and publish a notice on the Commissioner's website to that effect.

2.6 To be considered a Tier 1 service, "basic online safety requirements" must be in place, as set out at s.21 of the Act. This includes having terms of use that prohibit the posting of cyberbullying material, a complaints scheme for the reporting of cyberbullying material if terms of use are breached and a designated contact person for the Office to report matters to.

Tier 2

2.7 A social media service may be declared a Tier 2[1010] service on the recommendation of the Commissioner. To make a recommendation, the Commissioner must be satisfied that the service is a 'large social media service', or that the service has requested to be a Tier 2 service.

[1009] The following are a Tier 1 service: airG, Ask.fm, Flickr, musical.ly, Roblox, Snapchat, Twitter, Yahoo!7 Answers, Yahoo!7 Groups, Yubo.

[1010] The following are a Tier 2 service: Facebook, Google+, Instagram, YouTube

2.8 In cases where cyberbullying material has been posted on a Tier 2 service, the Commissioner may issue that service with a written notice requiring the service to remove the material within a 48 hour period. Failure to comply with a notice may lead to enforcement action being taken.

Discretionary powers

2.9 The Office has a broad range of discretionary powers and civil penalties under the Act, which enable it to take a range enforcement actions against individual perpetrators or the sites themselves. This includes fines of up to $21,000 a day for Tier 2 social media sites that do not comply with take down notices. While this may be pocket change for some of the big tech behemoths, the significance of this reputational impact for the social media companies, at this time, should not be underestimated. As has already been highlighted, the Office has received 100% compliance from industry to-date.

2.10 The Office can also issue an end-user notice, under s.42 of the Act, to a person that posts cyberbullying material, requiring them to take all reasonable steps to ensure the removal of the material, refrain from posting any cyber-bullying material targeting a child, and apologise for posting the material.

Mental Health Support and Referral

2.11 The Office also refers children and young people to dedicated support services, including counselling. The Office has partnered with the Kids Helpline, which has specialist expertise in dealing with children who encounter online bullying. We have currently referred over 6,000 young people to the Kids Helpline.

Statutory Review of the Act

2.13 The Act has a built-in opportunity for review, to ensure that there are proper regulatory controls and support systems in place to allow Australians to confidently take advantage of the benefits of the digital environment. Section 107 of the Act states that within three years after the commencement of this section of the Act, the Minister must cause to be conducted a review of the operation of the Act and whether the Act should be amended. This section also requires that a report be prepared, and tabled in each House of the Parliament within 15 sitting days after the completion of the report. The review must commence by 1 July 2018.

3. Online Content Scheme and CyberReport Team

3.1 The Office administers the Online Content Scheme, which allows Australian residents and bodies corporate to report illegal and offensive online content to the eSafety Commissioner. The Commissioner has the authority to direct the relevant content service provider to remove the content from their service and to take action on material it finds to be prohibited or potentially prohibited, as set out in

Schedules 5 and 7 of the Broadcasting Services Act of 1992. These prohibitions are backed by strong sanctions for non-compliance including criminal penalties for serious offences. The scheme provides important community safeguards, as well as dovetailing with the role of law enforcement and the international community of Internet Hotlines, known as INHOPE. The Office is the sister organisation of the UK's Internet Watch Foundation, and collaborates closely with the international community (for example, with NCMEC, Interpol and the WeProtect Global Alliance) in order to harness and promote innovation, investment and commitment to address and combat the proliferation of online child sexual exploitation.

3.2 The Office prioritises taking action on child sexual abuse material. Where such material is found to be hosted in Australia, the Office liaises with the relevant law enforcement agency to ensure that any action taken will not adversely impact ongoing police operations; the content is formally classified by the Classification board; and finally the Office formally directs the hosting company to remove the content. The Office works within a timeframe of two business days to have child abuse material removed, working hard to prevent the spread of child sexual abuse material and the re-victimisation of the young people who are the subject of these images.

3.3 In cases where child abuse content is hosted overseas, the Office either refers the content to the Australian Federal Police, or directly to an INHOPE member hotline in the hosting or production country. The key to the Office's success is close collaboration with internet, technology and payment industries and law enforcement. Since 1 July 2017, the CyberReport team has completed a total of 8,284 investigations. More than 60% of these (5,300) were assessed as child sexual abuse material (CSAM), and each was referred to law enforcement partners for take down.

Functions of the Online Content Scheme

3.4 Schedules 5 and 7 of the *Broadcasting Services Act 1992* (Cth) establish a regulatory scheme, commonly known as the 'Online Content Scheme'. Oversight of the Scheme transferred to the Office on 1 July 2015, and allows Australian residents and bodies corporate to report illegal and offensive online content to the eSafety Commissioner.

3.5 The Scheme provides the eSafety Commissioner a number of tools to regulate the internet and content industry, with the aim of protecting consumers, particularly children, from exposure to inappropriate or harmful material.

Schedule 7 provides that the Commissioner may issue:

- take down notices in cases involving a hosting service
- service-cessation notices in cases involving a live content service
- link-deletion services in cases involving a links service

3.6 Both Schedules 5 and 7 enable the eSafety Commissioner to:

- request that body or association of the internet and or content industry develop an industry code that applies to participants of their industry. Compliance with such codes are voluntary unless the Commissioner otherwise directs
- impose an industry code on the internet and or content industry in certain circumstances, including where a code has been requested but the request has not been complied with. Compliance with industry codes are mandatory.
- make a determination that applies via a legislative instrument to the internet and or content industry.

3.7 The Commissioner has the authority to direct a relevant content service provider to remove content from their service, and has powers to take action on material it finds to be prohibited or potentially prohibited. These prohibitions are backed by strong sanctions for non-compliance, including criminal penalties.

3.8 The Office prioritises taking action on child sexual abuse material within a timeframe of two working days with a view to having the material removed. Where material is found to be hosted in Australia, the Office liaises with the relevant law enforcement agency(ies) to ensure that action taken will not adversely impact ongoing police operations.

3.9 In cases where child abuse content is hosted overseas, the Office either refers the content to the Australian Federal Police, or directly to a relevant INHOPE member hotline. The key to the Office's success is close collaboration with internet, technology and payment industries and law enforcement.

3.10 To decide when content is likely to be prohibited under the *Broadcasting Services Act 1992 (Cth)*, the Office refers to the national Classification Scheme. Formal classification by the Classification Board is required before online material is definitively regarded as prohibited.

4. Image-based abuse portal

4.1 Image-based abuse – the sharing, or threatened sharing, of intimate images or videos without consent - is a terrible form of abuse and can have serious impacts on victims. (We prefer the term 'image-based abuse' to 'revenge porn' as it better reflects the range of motivations and behaviours we see and we should not shy away from describing it as 'abuse'.)

4.2 1 in 5 Australians have had their intimate images or videos taken or shared without their consent. In order to offer tangible support to Australians who have experienced image-based abuse, the Office launched its image-based abuse portal in mid-October 2017.

4.3 The portal is a place where Australians can report image-based abuse to seek its removal, and access practical advice and resources to help them manage the impacts of image-based abuse.

4.4 In the first six months of operation of the portal, the Office received over 180 reports of image-based abuse, and was successful in having image-based abuse material removed in 80% of cases. We had over 64,000 total visits to the portal in the same period.

Our report resolution approach

4.5 The Office has a three-pronged approach to responding to reports of image-based abuse. We make sure the victim is safe and supported, seek rapid removal of content, and keep the victim informed of our actions and progress.

4.6 We ensure highly distressed victims are immediately referred to an appropriate counselling or support service and if we're concerned the victim's personal safety is at risk, we help them collect evidence and refer them immediately to their local police. While requesting rapid removal of image-based abuse material is our primary role, we never lose sight of the fact that victims of image-based abuse have a range of needs. So, we also ensure that victims are connected with other appropriate services, such as expert counselling, legal assistance and family and domestic violence support services.

4.7 Where the abuse concerns under 18s and can be characterised as cyberbullying or child sexual abuse material, the Office relies on its current legislative powers. This has been leveraged to request that sites and hosts remove the material, regardless of the age of the victim.

4.8 The Government's proposed civil penalty scheme, set out in the *Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Bill 2017* is currently before Parliament. If passed, this should increase the Office's effectiveness in having image-based abuse material removed. The bill seeks to introduce a prohibition on the posting, or threatened posting, of intimate images and establish a complaints and objections system that the Office will administer. It would provide us with a diverse range of powers to enforce the statutory prohibition on the non-consensual sharing of intimate images, including the ability to give formal removal notices to websites, hosting providers and perpetrators.

4.9 The Office continues to innovate and develop tailor-made materials and programmes to address the online safety needs of a wide range of vulnerable communities. Examples of these efforts may be found at www.esafety.gov.au.

We would be pleased to answer any further questions the House of Lords might have about the function of the Office, our education and awareness programmes or the various schemes we operate.

9 May 2018

Stephen Oliver – written evidence (IRN0058)

1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

1. It is not possible to regulate the Internet as such. The Internet is merely a means to allow connections between computers connected to the Internet in order that data can be transferred from one to the other in either direction.

2. There are of course companies that provide access to the Internet. ISP's and telecommunications companies. They are already regulated. It is desirable that regulation of these businesses ensures net neutrality and the privacy of users' data. I suspect that the infrastructure of the Internet within the European Union functions more or less adequately but probably not in most other parts of the world. It is vitally important that telecommunications companies and ISPs provide open transparent services to allow individuals to connect to the Internet.

3. If you mean websites. Websites are merely publications on the Internet. Publishing is subject to regulation and the Common Law. The real problem that you are wrangling with is that certain websites have been granted immunity, as is acknowledged in this call for evidence. This has created monsters that have effectively annexed freedom of expression to spread disinformation and exploit all users of the Internet to make money by devious and nefarious strategies.

4. The urgent need is to revisit the legislation that grants immunity to websites for third party content. An ISP is a "mere conduit", a website isn't ever.

5. Advertising and Marketing, on the other hand, should be very heavily controlled and regulated so that it is always open and transparent.

6. The problem has arisen because EU and domestic legislation has followed the pattern of legislation in the USA. Congressional legislation is shaped by "lobbying". Lobbying is a synonym for bribery. Private Capital in the US saw that the advent of the Internet meant that it would not be possible to own and control monopolies on publishing and broadcasting when anyone could be a publisher. They realised that producing content would no longer be particularly profitable, whereas owning the vehicle for self publishing offered undreamt of opportunities to exploit the new audience.

2. What should the legal liability of online platforms be for the content that they host?

Stephen Oliver – written evidence (IRN0058)

1. Online "platforms" don't exist. A so-called "platform", such as Facebook or Youtube, is a website. Full stop. A website is a publisher. It should not be entitled to any special status as an "Information Society Service". The protections allowed to Information Society Services as "mere conduits", by the Electronic Commerce (EC Directive) Regulations 2002 in the UK, and EU Directive 2000/31/EC, should be limited to ISPs and telecommunications infrastructure companies. Publishers of websites should be liable for the content published no matter how it is sourced, in exactly the same way as a publisher in print is liable.

2. Anyone can publish a website on the Internet. All you need is some code stored on a computer, referred to as a "server", connected to the Internet so that it is accessible to any other computer, referred to as a "client". Dependant on the quality of the Internet connection and the code stored on the connected computers, a client computer is more or less the same as a server computer. That is what is so revolutionary about the Internet. Anyone can connect to anyone else without the need for some giant corporation to mediate that connection. Everyone can be a publisher.

3. Anyone with only some knowledge of open source programmes, and no coding skill at all, can set up a website to allow third parties to post content in a few hours for the expenditure of maybe $50.

4. Publishing began with Gutenburg and Caxton. Over the centuries a lot of Common Law and legislation has developed around publishing. Why should an online publisher be immune? Why should it matter whether the content is sourced by writing it yourself, by paying someone to write it for you, through syndication, or inviting unpaid contributions from readers, or publishing paid for advertisements? Why should it matter whether the publisher reads or edits the content before he publishes it? To publish something without exercising very much editorial control over it, is an editorial decision in itself. It's not as if the publishers of Facebook allow the contributor to publish anything just as they like, to remove the Facebook logo and replace it with their own for instance. Or post the content in a place reserved for Facebook's terms of service, or anywhere but in the place provided by Facebook, in Facebook's template.

5. If I write a letter to the editor of a newspaper, and it is published, the newspaper is liable if it contains a libel equally with myself. For this reason newspapers are careful not to publish letters which might be actionable. This is not a restraint of my freedom of speech. I am free to send a copy of my letter to whomsoever I please. Print handbills and hand them out in the street. Or publish it as a website. But though I am free to do so, I do so at my own risk. It cannot be in the public interest that I could publish the same libel on Twitter or Facebook, more or less anonymously, and the publisher would not be liable. You don't need to be particularly clever to set up a profile under a bogus identity on such a website. Twitter or Facebook will potentially publish that libel to millions of

other persons, far more than a print newspaper could reach, and vastly more than you could hand out handbills to. But Twitter or Facebook is immune from liability if they take it down upon complaint within certain time limits. But that is after the damage is done. So the reason they don't edit the content they publish is that it would cost time money and effort to do so. There's no risk or downside to publishing everything, whether the content infringes copyright, is defamatory, or illegal in other ways. They don't even need to pay for newsprint to accommodate the acres of drivel, libels and infringements they publish.

6. I am a big fan of Article 10 of the European Convention on Human Rights. And as far as free speech is concerned my attitude is the similar to the famous apocryphal saying attributed to Voltaire. I am though particularly conscious of the second paragraph of Article 10, which begins: "*The exercise of these freedoms, since it carries with it duties and responsibilities,…*" The problem of so-called social media and the monolithic companies that have annexed popular access to the Internet is that they are exercising freedom of expression with flagrant disregard to the duties and responsibilities that freedom of expression requires. At the same time the business model of these organisations is essentially criminal. They are founded on theft and the exploitation of their users.

7. If all websites were liable in the United Kingdom in the same way as print publishers the social media websites would not be able to continue with their current model to users within the United Kingdom. There would be an outpouring of anguish that might last a week or a fortnight or so. But better more democratic models of Internet connectivity would replace them within a very short time. People would adapt to paying to host their own content on the Internet and maintaining their privacy.

11 May 2018

Open Data Institute – written evidence (IRN0073)

This is the response from the Open Data Institute (ODI) to the House of Lord Select Committee on Communications call for evidence into internet regulation. The ODI is a global not-for-profit which is headquartered in London.

The ODI's response is focussed on data and openness. Our vision is for people, organisations and communities to use data to make better decisions and be protected from any harmful impacts. We work with governments and businesses around the world to deliver on this vision.

1. *Is there a need to introduce specific regulation for the internet? Is it desirable or possible?*

1.1. It is important to note that the internet is many-layered including physical hardware both for the last mile to homes and offices, as well as the interconnections between networks and nation states; protocol layers such as TCP, UDP and DHCP; through to more visible layers such as the web, the advertising ecosystem and consumer-facing services such as Facebook, Google and BBC iPlayer. Our response is focussed on data and how it flows around the more visible layers of the web.

1.2. There are already numerous pieces of regulation that impact the internet, for example data protection and anti-discrimination regulation. These have evolved over the last few decades and will need to evolve further. The possibilities provided by technology are constantly changing, as are people's needs and expectations.

1.3. It is important to be reasonably precise about the desired outcome of new regulatory interventions before they are designed. To deliver on the ODI's vision of better use of data may make require nations to implement regulation to help build data infrastructure that is as open as possible while respecting privacy and to build on the EU GDPR and UK Data Protection Bill to gradually create a stronger rights framework for data[1011]. These regulatory approaches will support innovation while maintaining trust from citizens and consumers.

2. *What should the legal liability of online platforms be for the content that they host?*

2.1. No response.

3. *How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who*

[1011] https://oldsite.theodi.org/blog/what-would-legislation-for-data-infrastructure-look-like
https://theodi.org/article/no-one-owns-data-we-need-to-strengthen-our-rights/

wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

3.1. No response.

4. *What role should users play in establishing and maintaining online community standards for content and behaviour?*

4.1. No response.

5. *What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?*

5.1. If online platforms, or any other organisation, are providing all or part of a public service then they should provide the same right to freedom of information and compliance with government's open data policies as public sector organisations. This supports innovation and accountability and is in line with the UK's commitment to and support for the Open Government Partnership[1012].

5.2. The UK Government should be strengthening its legislation and procurement rules to help deliver on this objective.

5.3. The European Union is discussing current regulations on this topic as part of an update to the Reuse of Public Sector Information (PSI) directive[1013]. Their work may be useful to inform further work by the UK Government.

6. *What information should online platforms provide to users about the use of their personal data?*

6.1. We should be careful of the trap of personal data ownership and property rights. While many users believe that data about them is 'theirs' and that they 'own' it, a rights framework is a better long-term approach to create the most social and economic value from data in ways that people trust[1014].

6.2. All organisations should start with the overarching goal of being open about how personal data is collected, shared and used. This will help create trust and allow scrutiny by both individual users and the organisations, such as consumer rights organisations, that support them in making decisions or that hold them to account when things go wrong. These support organisations are necessary. The general public's confidence in and understanding of data is low as shown by recent surveys by ourselves and detailed research by DotEveryone[1015].

[1012] https://www.opengovpartnership.org/

[1013] https://ec.europa.eu/digital-single-market/en/proposal-revision-public-sector-information-psi-directive

[1014] https://theodi.org/article/no-one-owns-data-we-need-to-strengthen-our-rights/

[1015] https://theodi.org/article/odi-survey-reveals-british-consumer-attitudes-to-sharing-personal-data/
http://understanding.doteveryone.org.uk/

6.3. We have developed a set of principles which expand on the goal of openness about personal data being used and would encourage the committee and government to do more to provide basic data literacy across the population and in providing support for third parties that support citizens[1016].

6.4. While we need to ensure that all of this information about how data is collected, shared and used is openly available, in many contexts users will need a more limited set of information to help them make a particular decision about what data to share (for example, "should I allow this third-party access to bank account data?"). The needed contextual information will vary by organisation and by decision. This should form part of the design process for particular services offered by any organisation.

6.5. Online platforms should also respect people's rights and provide them with access to information about themselves and the ability to port it to other providers. This could help create a more competitive market, help protect people's privacy and support the creation of innovative new services. Government plays a role in helping to make this happen[1017].

6.6. While respecting the rights of individuals, government should also consider group rights, for example the groups of people example the two or more people in a social media conversation, as explored in a recent report by the ODI and IF[1018]. Group rights are an emerging area of research which may form part of the next round of data legislation after GDPR. The research needs support from governments and businesses along with practical exploration and prototyping of a next generation of services with consumers and citizens.

7. *In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?*

7.1. Building trust in business practices in the way that data is used is more than a regulatory burden, it is an opportunity - as shown in our recent report on artificial intelligence business models[1019]. Trust in how organisations use data is increasingly being seen as a competitive advantage and a point of differentiation. Transparency and openness is a vital way to build trust.

7.2. Practical tools like the ODI's Data Ethics Canvas can help organisations to both make better decisions and be more open about their approaches[1020].

8. *What is the impact of the dominance of a small number of online platforms in certain online markets?*

[1016] https://theodi.org/article/openness-principles-for-organisations-handling-personal-data/

[1017] https://theodi.org/article/data-portability-the-role-governments-should-play/

[1018] https://www.legislation.gov.uk/ukpga/2010/15/section/4 https://dataportability.projectsbyif.com/ https://linnettaylor.wordpress.com/2017/01/10/group-privacy-a-new-book-on-the-next-generation-of-privacy-problems/

[1019] https://theodi.org/article/the-role-of-data-in-ai-business-models/

[1020] https://theodi.org/article/updating-the-data-ethics-canvas/

8.1. While it is not the only impact created by their dominance, we are primarily concerned by how larger online platforms have control over large data assets and the attention of users who help to maintain and improve those data assets through their use of the online platform's services. This control limits how that data is used, reducing innovation and competition.

8.2. We believe that increasing access to data, both that held by the public sector and that held by the private sector, will help level the playing field and create a fairer and more equitable market with social and economic benefits for consumers, citizens and society as a whole[1021].

8.3. In addition, because people do not feel they have a choice about using these platforms, they may adopt practices such as providing false data, which they then adopt in other circumstances (such as online public services). These practices could undermine the quality of data in other situations, and the quality of decisions based on that data.
with protected characteristics under the Equalities Act, and where there might be competing interests between groups of people identifiable in, or impacted by, data, for

9. *What effect will the United Kingdom leaving the European Union have on the regulation of the internet?*

9.1. It is easier for large businesses to operate in multiple compliance regimes than the startups and SMEs that are necessary to drive innovation and who will create future trade exports and inward investment. The UK Government has said that it wants to implement data legislation which is equivalent to that deployed by the European Union and to seek an equivalence agreement which allows data to flow freely between the EU and UK. For the UK Government to deliver on its goal of a thriving digital and data ecosystem then, as TechUK have shown, it is vital that data equivalence occurs and that the free flow of data continues.[1022]

9.2. While some types of legislation and interventions will work at a national level, there are others which will need support from multiple nations or even globally through bodies such as the United Nations before they will have significant impact on the global internet ecosystem.

9.3. Different nations have different needs and goals. Different societies are moving at different velocities, and sometimes in diverging directions, as we adapt to the current information age.

[1021] http://www.jenitennison.com/2018/01/14/data-monopolies.html

[1022] http://www.techuk.org/insights/news/item/11824-rapid-action-needed-to-safeguard-uk-eu-businesses-consumers-following-brexit

9.4. As the UK leaves the EU it will it needs to ensure that it retains strong bonds with a group of nations whose societal expectations and needs of technology are evolving at a similar pace and in a similar direction and are willing and able to intervene to deliver multinational regulation.

May 2018

Open Rights Group – written evidence (IRN0090)

Summary

Our primary point is that users have a *right to publish* and need the ability to *take legal responsibility for their work* when it is identified for removal; and that systems of issuing *notice to platform and user* and *counter-notice to the platform and complainant* ("*notice and counter-notice*") provide a basic framework to achieve this. However, with the exception of libel law, these systems do not exist in the UK and EU. Additionally, the current framework already makes platforms liable for content when they are notified; this leaves users in a vulnerable position where they cannot defend their publications on platforms.

We also detail ad-hoc regulation by Police, Nominet and UK law enforcement agencies to remove content and domain names which lack accountability and oversight. A further 'quick win' would be for bodies that deal with Internet regulation, including the BBFC, IWF, National Crime Agency, and National Trading Standards to be brought within the scope of Freedom of Information legislation, and for Nominet to introduce an independent appeals process for domain suspensions.

(ii) 1a. Is there a need to introduce a new regulatory framework for the Internet?

Arguably, the current regulatory systems that constrain the internet already function reasonably well.

Data protection, e-Privacy, electronic commerce and defamation laws serve different and extremely important purposes. Laws of course evolve and more protection for privacy is particularly needed, as are protections for the right of users to publish lawful content. In practice, there is not enough scope within current legal frameworks to protect users' right to publish on platforms and few systems of *notice and counter-notice* exist to allow users to take legal responsibility when their content is challenged.

Internet regulation is a complex web of various stakeholders and laws which interact with each other through a multistakeholder governance model. As the Internet is not a single entity and is comprised of tens of thousands of private actors, it would be difficult to establish a single new framework for regulation.

Laws must be targeted in scope towards a particular problem or set of problems, as the necessary complexity of legislation will depend on what is being regulated. The wider the scope of a particular piece of regulation, the simpler and less specific it is going to be. For example, the Electronic Commerce Directive (ECD) protects platforms and intermediaries against incurring liability for the actions or users. It is a critically important piece of law but is very simply drafted. Similarly, data protection laws are very important but are drafted very widely as they are unable to address the narrow and particular privacy risks seen by specific industry sectors. Current debate in this area appears to be focused on the role of large platforms like Facebook and Google, evaluating what kind of role they can play in policing online content. This effectively involves eroding their liability protections by creating a looming threat of more formal regulation if they do not take action to remove unwanted content.

From a user's perspective, ensuring that online platforms are protected from liability is critically important. A user's right to publish and to defend their legal right to publication is critical to the open web. When the law does not properly recognise the right of users to defend this right to publication, we experience arbitrary censorship.

Often the Internet and platforms are identified as a politically acceptable arena in which to intervene, without regard to the effectiveness of that intervention. Policy makers at all times can focus on platforms; persons creating a problem; or other social factors that generate the behaviour. Of the three, platforms may be the easiest to push into taking action, but this is likely to be less effective in real terms than dealing with the people or criminals directly, or taking action to deal with root causes. Instead, platforms are treated as a root cause, even though this is rarely the case.

1) Necessity

The question above, which regards the perceived *need* to regulate the Internet, explicitly references the test of *necessity*. Necessity is the legal principle that any new law should be capable of being justified from an objective perspective.

This is defined within the context of personal data protection by the European Data Protection Supervisor (EDPS) as follows. Although this definition comes from data protection law, it also applies more generally:

> "Necessity is a fundamental principle when assessing the restriction of fundamental rights, such as the right to the protection of personal data. According to case-law, because of the role the processing of personal data entails for a series of fundamental rights, the limiting of the fundamental right to the protection of personal data must be strictly necessary.
>
> Necessity shall be justified on the basis of objective evidence and is the first step before assessing the proportionality of the limitation. Necessity is also fundamental when assessing the lawfulness of the processing of personal data. The processing operations, the categories of data processed and the duration the data are kept shall be necessary for the purpose of the processing."

The legislature must be satisfied that any proposed Internet regulation is necessary before moving on to consider the test of proportionality.

In questioning whether a piece of legislation may meet the test of necessity, the Government should consider whether the regulation of a particular platform or of the Internet is *necessary* to achieve the goals of the legislation. We are aware that this Committee heard recently of the issues surrounding the FOSTA and SESTA legislation in the United States. FOSTA and SESTA sought to address some of the real-world problems presented by sex trafficking through the regulation of online platforms. The regulation of the platforms does not solve these problems, and can only serve to make them worse.
Instead of seeking the 'easy solution' of placing sanctions on online platforms, lawmakers should attempt to tackle issues head-on. Addressing the problems Congress had identified with sex trafficking should have taken part as part of a broader policy discussion focusing on those issues, rather than deferring such problems to online platforms to solve, by making them liable for anything that could constitute "facilitation" of sex trafficking.

Following FOSTA and SESTA, sex workers as a whole are now unable to advertise for clients online using platforms which had been established for many years and had community reputations. With the loss of these avenues for advertising, sex workers are being forced to soliciting clients on the street, which is far more unsafe, and leaves Congress with less of an ability to control the situation.[1023] A study published in November 2017 by the universities of Baylor and West Virginia highlighted that in cities where Craigslist had opened online boards for advertising erotic services, the rate of homicide *against women in general* fell by 17 percent.[1024]

In the US case, this problem will affect many sex workers in the UK and elsewhere, as they will be unable to use US-based platforms. Nevertheless, over 76,000 Twitter users, for instance, recently signed up to an Australian Twitter-style service called Switter,[1025] which aims to cater to sex workers and clients.[1026] This illustrates the difficulty of simplistic bans. In any case, while the aim of FOSTA and SESTA was to tackle sex trafficking, the impacts have been on sex workers as a whole. It would be hard to imagine a ban on migratory farm workers using Internet platforms as the result of concerns about forced labour and modern slavery, yet this has been a politically acceptable approach in this case.

Proportionality

Proportionality is also defined within the context of personal data protection by the European Data Protection Supervisor (EDPS) as follows:

> "Proportionality is a general principle of EU law. It restricts authorities in the exercise of their powers by requiring them to strike a balance between the

[1023] https://motherboard.vice.com/en_us/article/bjpqvz/fosta-sesta-sex-work-and-trafficking
[1024] http://gregoryjdeangelo.com/workingpapers/Craigslist5.0.pdf
[1025] https://switter.at
[1026] https://medium.com/assembly-four/my-six-week-rollercoaster-ride-172eb58ba80e

> means used and the intended aim. In the context of fundamental rights, such as the right to the protection of personal data, proportionality is key for any limitation on these rights."
>
> "More specifically, proportionality requires that advantages due to limiting the right are not outweighed by the disadvantages to exercise the right. In other words, the limitation on the right must be justified. Safeguards accompanying a measure can support the justification of a measure. A pre-condition is that the measure is adequate to achieve the envisaged objective. In addition, when assessing the processing of personal data, proportionality requires that only that personal data which is adequate and relevant for the purposes of the processing is collected and processed".

A clear case of disproportionality can be found in the UK's Digital Economy Act 2010, which proposed suspending access to the Internet for ISPs' users who had received three allegations of downloading copyright infringing material. Account suspension could have disrupted education, job seeking and access to government services for whole families and seemed wholly disproportionate.

In this case, online copyright infringement was held by lobby groups to be so severe that TV, video and music industries simply could not compete against 'free' services. This was delayed and did not take place.

Thankfully, the plan was never put into action, and the problem has subsequently been resolved through proper supply of services such as Netflix, Amazon Prime, BBC iPlayer, Spotify, Deezer and others. The market has reduced infringement primarily through the supply of good services, as we suggested it could at the time. The calls for 'urgent' regulation of the Internet could have resulted in serious harm for individuals and, though heeded in 2010, were pushed into the long grass.

Is it desirable?

Clearly the child protection imperative with regards to child pornography (Indecent Images of Children as defined under the Protection of Children Act 1978) is necessary and proportionate in a democratic society.

However, other technical infringements of freedom of expression must also be demonstrably necessary and proportionate; and consideration of the impact of regulation on communities who receive information, as well as the individuals who impart it, must be given.

Is it possible?

This question raises the spectre of practical workability.

For example, the current age verification régime, as dictated by the Digital Economy Act 2017, has been acknowledged as unworkable in practice; in the sense that it is easy to obviate using tools such as Tor, Virtual Private Networks (VPNs), or proxies.

Given the current rate of technological development, it seems likely that advances which allow tech-literate users to simply "get round" regulation will continue apace.

1b. In your view, should we encourage self-regulation or employ more directive means such as co-regulation or direct (command and control) regulation?

We have concerns that self-regulation in practice often consists of Government forcing the hands of platforms by making platforms feel that they have to take steps to regulate of their own volition, otherwise they will face legislative regulation for which there may be sanctions or penalties for failure.

This leads to a culture of "privatised enforcement", where the will of Government is carried out by private actors under a self-regulatory framework. The lack of a threat of penalties or sanctions for failure means that there is a lack of incentive for platforms to invest the necessary resources into getting things right.

Fundamentally, this is about how we deal with crime and victims. Encouraging an entirely self-regulatory regime risks the danger that we give up on the direct enforcement of criminal activity and merely try to disrupt the criminal activity online rather than pursuing criminals. This is due to the fact that platforms can *only* disrupt and have no law enforcement powers. Facebook and Google do not operate courts or prisons. Direct enforcement action against criminal activity should not be something that is lost track of when considering alternative forms of regulation.

In many situations - particularly some fraud, bullying, and harassment cases - relying on disruption tactics to remove offending posts and content from platforms results in criminals being left to go free where it is possible for them to be prosecuted. Determined criminals and serial bullies or harrasors are free to continue what they are doing.

Of course, it must be recognised that the Internet is a global network, and it is not always possible to take action beyond disruption if perpetrators are located outside of the UK. However, if offenders are based in the UK or other legally-cooperative countries then this should not be the case.

In response to this question, we can also consider the failures of self-regulation when it comes to privacy. One example is mandatory cookie warnings and online advertising; a complete failure of industry self regulation. Most cookies don't need a banner and when they do there is not enough info.

2. Should online platforms be liable legally for the content that they host? In your view, are online platforms publishers or mere conduits?

Online platforms and liability for the content they host

The general legal position is that online platforms are currently liable for hosting unlawful content if they do so knowingly, though defences are available if the platform does not know they are hosting the content.

In current EU law, liability defences are not attached to an entity, but to specific content and actions. An online newspaper running uncurated comments below articles will generally receive protection from potential liability arising from what their users write. Similarly, an online platform which generates its own content will not be afforded the same liability protection.

The main liability protections for online platforms currently come from the Electronic Commerce Directive, implemented domestically as The Electronic Commerce (EC Directive) Regulations 2002. As "hosting" providers, platforms are currently offered protection from liability under Article 14 ECD. Platforms are neutral providers that host the content of third parties and users, but do not generate the content themselves or undertake editorial decisions.

An exception for persons acting as a "mere conduit" - as this question refers to - can be found in Article 12 ECD, although it should be noted that this refers primarily to Internet service providers and other intermediaries who do not store the content they are transmitting and is thus not the correct term to use when discussing online platforms.

Libel

More specifically, when dealing with libelous content, additional protections are available for platforms in England and Wales under the Defamation Act 2013.[1027] Under the Act, it is a defence for a platform operator to show that they were not the person who posted the defamatory statement on the website. Liability for defamatory comments rests with the originator of the comment.

The Defamation Act outlines a system of *notice and counter-notice*, which allows an original poster of a potentially defamatory statement to defend their right to publish. This applies where the original poster consents to their personal details being passed back to the complainant.

This should serve as a model for the other areas of law we have identified in this document as lacking any similar mechanism.

Patent law

The main law surrounding patents in the UK can be found in the Patents Act 1977.

[1027] Defamation Act 2013, s.5

Once again, the general liability exemption that might apply here, for ISPs and platforms, are the Electronic Commerce Directive exemptions for "caching", "hosting" and "mere conduit". It is worth noting that the "hosting" exemption only applies where a provider does not have "actual knowledge" that they are hosting unlawful content. Once a notice is received, the hosting platform is liable for the content.

UK law also provides a statutory right of redress against unjustified or groundless threats to sue for patent or trade mark infringement. According to the Law Commission, "If a threat to sue for infringement is made where there has been no infringement, or the right is invalid, it is said to be groundless or unjustified. Any person aggrieved, that is whose commercial interests suffer because of the threat, may apply to court for a remedy. These are an injunction to stop the threats, a declaration that there has been no infringement and/or damages for loss caused by the threats."

The default position of the law in favouring online platforms presents difficulties for UK businesses who sell goods through the eBay platform who have their listing removed through notice by third parties in response to allegations of patent infringement.
We have seen this clearly with our campaign against printer manufacturer Epson's tactics in persuading eBay to remove store listings for third-party ink cartridges which fit Epson printers. As a trusted member of eBay's Verified Rights Owner (VeRO) programme, Epson was taken at their word over a highly technical patent claim while the accused were denied a proper chance to defend themselves.[1028]
eBay are in a difficult position, as they cannot realistically assess a patent claim, nor can they pass the legal responsibility to the person making the listing.

Here, a system of *notice and counter-notice* would allow eBay's customers to assume legal responsibility. Ebay would notify the customer of a complaint; the customer would file a counter-notice in which they would assume legal responsibility for the listing. The customers' details would be passed to Epson, so that Epson and the cartridge reseller could resolve the issue between themselves, if necessary in a court.

Without a legal framework, this is not an option.

Trade mark law

A trade mark is a graphical sign used to distinguish one party's goods or services from those sold by others. To protect their brand or image, the owner of a trade mark is granted the power to seek legal remedies if another party makes use of that mark in the course of trade.

[1028] See our campaign at: https://epsonstopkillingcompatibles.org.uk/; also https://wiki.openrightsgroup.org/wiki/Epson/Patent_takedowns; and https://wiki.openrightsgroup.org/wiki/Epson for background.

A person can protect their trade mark by registering it with the UK Intellectual Property Office (UKIPO), which makes legal remedies for infringement available under the Trade Marks Act 1994. If a trade mark is not registered, then some protections may still be available under the common law of 'passing off'.

Where a person's trade mark is infringed via an online platform - for instance, by a user of an online marketplace site offering counterfeit goods for sale - the trade mark owner may generally only take action against the party who is posting the content and not the platform itself. The operator of a service will generally be entitled to rely on the 'hosting' exemption of the Electronic Commerce Directive to indemnify themselves from liability.

As per the wording of the Electronic Commerce Directive, the service's liability exemption for 'hosting' ceases to apply if they are presented with "actual knowledge" of trade mark infringement happening on their platform. When presented with this knowledge, a provider would have to take action to remove the infringing content.

A service operator also cannot rely on the 'hosting' exemption if their service does deal with the trade mark infringing content in a neutral manner. If the operator can be said to have taken active steps with the content that would give it knowledge, or control over, the data stored. This is confirmed by the cases of L'Oréal, and Google v Louis Vuitton.

The case of Cartier, also confirms that patent-holders have the right to request that a court order ISPs in the UK to block websites which are infringing their trade marks and selling counterfeit goods. A pending judgment in the case from the UK Supreme Court will confirm whether ISPs are required to bear the cost of implementing the blocking for such sites.

Copyright

In the UK, DMCA rules have often substituted for a codified legal process of *notice and counter-notice* for copyright claims. For instance, Youtube videos that are produced for use in the UK may receive copyright violation notices, which can then be contested by the UK user by agreeing to the jurisdiction of US courts and allowing their personal details to be passed.

This is dissatisfactory for a number of reasons, but in particular, a UK hosting company cannot legally allow users to provide a '*counter notice*'. Instead, the UK host must either remove the content, or accept legal liability for it under the terms of the e-Commerce Directive, as they may have 'actual knowledge' as the result of notification.

This is the case with eBay. Again, under the terms of their VeRO programme, a rights holder can remove anything they like from eBay if they claim it violates their copyright. The reseller at eBay cannot contest this. eBay cannot rely on a DMCA *notice and counter-notice* system, because it does not exist in UK or EU law.

Current proposals in EU law (Directive 2016/0280 on the "Digital Single Market") would require all platforms to implement filters which would automatically detect copyrighted material being uploaded by users, and could take appropriate action to stop the content from being uploaded publicly. Such filters are wide-ranging and inaccurate and the potential for expression to be curtailed through the over-censorship of legitimate content is massive. There are many reasons why uploaded works may incorporate segments of others, such as criticism, review, or remixing. As it is currently framed, copyright holders are currently left to be the 'deciding voice' on whether the copyright filters are adequate and fit-for-purpose.[1029] It is also very hard to see how this proposal does not amount to 'general monitoring' of users' communications which is prohibited under Article 15 of the Electronic Commerce Directive.[1030]

Our concerns

We have concerns that, under the current regime, the shields protecting online platforms from incurring liability are too weak. As we have seen repeatedly through our work, it is very easy for content to be reported and face removal without the user being granted the ability to take responsibility for their own content through a standard system of *notice and counter-notice*.

Online platforms as publishers

The classification of platforms as publishers should be approached with caution. Publishers claim exclusive rights over their content, and act as much narrower gatekeepers. Reclassifying platforms in this way would lead to an extremely concerning chilling effect and would jeopardise the concept of an open Internet.

Even with the current imbalance, we see problems for UK businesses and free expression. Users do not have a right to defend their right to publication, except in limited circumstances. By adding liability for users content to platforms, those companies would have a direct disincentive to allow users to take legal risks at the platform or companies' expense.

Furthermore, there is no need to reclassify platforms as publishers if the desired outcome is to prevent a platform from 'hiding behind' the Article 14 hosting defence. As indicated by Article 14(1)(b) ECD, a provider who obtains, or is provided, "actual knowledge" of the fact that they are hosting unlawful content must act "expeditiously" to remove the offending content, otherwise they will be unable to rely on the exemption.

[1029] "Information society service providers that store and provide to the public access to significant amounts of works or other subject - matter uploaded by their users shall, **in cooperation with rightholders**, take appropriate and proportionate measures to ensure the functioning of agreements concluded with rightholders for the use of their works or other subject-matter." - https://ec.europa.eu/digital-single-market/en/news/proposal-directive-european-parliament-and-council-copyright-digital-single-market

[1030] For more information about our concerns with Article 15 ECD, please see: Appendix B: *Article 15 ECD Submission.*

3a. What processes do online platforms use to moderate content that they host? Are these processes fair, accountable and transparent?

The processes used by online platforms are opaque, unaccountable and unfair. We know very little about how their systems work, and what aspects of their moderation is automated, or involves humans. What criteria are platforms using? Who decides those criteria? Who arbitrates in decisions on borderline cases? What action can be taken, and who determines the action?

There is very limited information available to assist with answering the above questions.

Online platforms are not transparent about how they moderate, and do not offer accessible systems of redress for users to challenge moderation when it occurs.

3b. What processes are employed by law enforcement agencies and other bodies such as the Internet Watch Foundation in overseeing the regulation of online content? Are these processes fair, accountable and transparent?

In our research into these bodies, our preliminary conclusions are that they frequently operate with:

- A lack of accountability;
- Little to no oversight;
- No prior authorisation for content takedowns;
- Often no independent appeals, or no appeals at all;
- In many cases, such bodies are not subject to Freedom of Information requests, or rely heavily on the 'crime' or 'national security' defences to avoid responding to requests.

The following is non-exhaustive list of bodies with an interest in content regulation:[1031]

Current Regulatory Framework

Crime

[1031] This list is maintained at: https://wiki.openrightsgroup.org/wiki/UK_Internet_content_regulation

CTIRU: produces a single statistic of takedown requests. Appears to lack any formal oversight of their takedown requests and refuses any transparency relating to their work, applying FoI exemptions to everything they do. CTIRU also make requests for domain suspensions to Nominet, again without supervision.

National Police Chiefs' Council: has a role co-ordinating counter-terrorism police work, including that of CTIRU. The NPCC is not subject to the FoI Act although it does respond to requests.

Home Office: administering CTIRU's list of websites to block across the public estate, with no oversight of the list or where or why it is applied. No oversight of any potential monitoring or information flow relating to persons making visits to sites on the list. No oversight of relationships with vendors within the programme.

National Crime Agency: does some takedowns, entirely exempt from FoI. Unclear what if any oversight takedown or suspension requests require.

IWF: a private company and charity, lacking FoI obligations but acknowledging they act as a state authority when blocking child abuse material. Unclear what their current presentation of block pages is, and whether this is any help for victims, people thinking about breaking the law or correcting errors.

CPS: Prosecutes cases, on basis that can be unclear, despite guidelines.

General

Nominet: a private company, subject to DEA 2010 clauses that allow the government to disempower it in the event of it failing to meet public objectives. Not subject to FoI in relation to these public objectives. Transparent in general terms, but recently reduced transparency about its governance. No transparency surrounding the 16,000 domains suspended via PIPCU and others, except in numerical terms. No longer transparent in terms of governance.

Ofcom: subject to high levels of transparency and accountability, but as of yet no clear policy or accountability around Net Neutrality complaints and violations.

Consumer protection

PIPCU: subject to FoI, have been very co-operative in this regard. No formal oversight of their takedown work. Removing over 13,000 domains annually via Nominet. These are mostly related to trade mark violations, fake goods and fraud.

National Fraud Intelligence Bureau: makes domain suspension requests to Nominet. No formal oversight of these requests.

Veterinary Medicines Directorate of DEFRA: makes domain suspension requests to Nominet. No formal oversight of these requests.

Metropolitan Police Fraud and Linked Crime Online (FALCON): makes domain suspension requests to Nominet. No formal oversight of these requests.

Medicines and Healthcare Products Regulatory Agency (MHRA): makes domain suspension requests to Nominet. No formal oversight of these requests.

National Trading Standards: a private company not subject to FoI or external oversight, which coordinates local trading standards' work. Makes domain suspension requests to Nominet.

Gambling Commission: regulates gambling for the UK, and requires non-UK hosted Internet gambling to hold a license, which includes an obligation for age verification.

Intellectual property

IPO: the IPO supports PIPCU's work and has a role in their governance, as well as having a role in wider IP enforcement. Unclear if e-Commerce advice and policy development for IP takedowns are their remit, or a question for another body.

Court order blocks: these delegate responsibility for identification of duplicate sites for blocking to various private organisations with copyright or trade mark claims, such as the BPI or MPA. No oversight of transparency of the lists of blocked URLs (other than ORG's detection tools). No transparency over their role in error correction on block pages. Confusing block pages at ISPs.

FACT: FACT, the Federation Against Copyright Theft, have issued domain seizure requests to registrars and redirected domains to a redirect page.

Child protection

ISP Soft blocking: lacking any legal requirements for user choice, error correction or visibility of what is blocked. Probably in violation of net neutrality laws barring ISPs from interfering with Internet traffic.

BBFC: a private company, with statutory duties in different legislation. Acquires new duties for blocking under DEA 2017. Generally reasonably transparent, but not subject to FoI. Provides limited accountability for specific mobile operators' website blocks, and publishes reasons for decisions about specific complaints.

UK Council for Child Internet Safety: responsible for industry co-ordination, but often tasked with patching up problems generated by government-pushed policy, such as Internet filters. Transparent and subject to FoI, as a government initiative; but unclear in its accountability as its measures generally count as industry self-regulation.

Internet Matters: an industry-led initiative to educate parents in matters of child protection, but also provides advice to website operators about getting sites unblocked.

Are these processes fair accountable and transparent?

The processes employed by law enforcement agencies often do not focus directly on a criminal actor, but on innocent third party intermediaries, seeking to place liability on those intermediaries. They are rarely fair, accountable, or transparent.

Firstly, these processes are often shrouded in secrecy, with the excuse that revealing information about how they would would jeopardise effective law enforcement by allowing criminals to see when their content is being censored, or to learn how any blocks are implemented so they can be circumvented.

Secondly, law enforcement are increasingly turning to unofficial methods of censoring content, which are not performed under a particular statutory authority. Law enforcement appears to prefer to outsource such interferences with expression, as private entities are not curtailed by human rights laws when it comes to censoring speech on their platforms.

In our work, the notable examples we have encountered to illustrate the above points include the Counter-Terrorism Internet Referral Unit (CTIRU), and the Police Intellectual Property Crime Unit (PIPCU), and domain suspension enabled by Nominet.

CTIRU in particular cannot be said to be accountable or transparent. CTIRU's aim is to remove material promoting terrorism from the Internet. This is not done under any statutory authority and appears to consist of contacting platforms directly and requesting that they remove the content by notifying the platform in question that the content is in breach of the platform's own terms of service. ORG have submitted Freedom of Information Act requests to obtain more information about how CTIRU operates, but these requests have been persistently refused for national security reasons.

More recently, following an investigation by the ICO into one of our FoI requests, the Metropolitan Police Service stated that CTIRU *do not keep internal statistics* about their operations, except for their claim to have removed over 300,000 pieces of extremist content.[1032] This represents a major concern for accountability and transparency. Although CTIRU are not submitting statutory requests to remove content, they are a publicly-funded organisation whose aim is to remove content from the Internet, thus transparency and accountability should be paramount.

[1032] See Appendix A: *Letter from Metropolitan Police Service to Open Rights Group in response to Information Commissioner's Office inquiry into Freedom of Information Request.*

Furthermore, CTIRU 'requests' have the legal effect of removing liability protection at platforms by providing potential 'actual knowledge' of an offence. A decision by a platform to leave the content as published is to accept legal liability for it. This requires accountability. It should include the possibility for a user to accept legal responsibility for it, through a system of *notice and counter-notice*.

Additionally, it is unknown what a 'piece' of CTIRU content may mean. We suspect that one web page may involve many 'pieces' of content, and thus the 300,000 'pieces' of content may in fact be a much smaller number of web pages or web documents. For this reason we have asked CTIRU for their methodology via FoI.

PIPCU operate an "infringing websites list", which they share with advertisers in an attempt to prevent them from advertising on known "pirate" sites, so that they can starve the sites of income.

PIPCU's list is secret, and the Police claim that they do not force advertisers to withdraw their advertisements, and that any restriction on freedom of expression is therefore not their problem. Advertisers in turn claim that the responsibility lies with the Police for compiling the list and they are just doing their duty once they are informed.

PIPCU and a number of bodies, as listed above, are involved in a programme of *domain suspension* in cooperation with Nominet, the registry for all sites using the .uk country code top level domain.[1033] The number of domains suspended has doubled annually since 2015, now standing at over 16,000 a year. Nominet make the actual suspensions after notification by an agency that they are associated with criminal activity.

Appeals are directed back to the agencies who requested the suspension. There is no independent appeal process, nor any external oversight. Most of the agencies have no published policy about when and why they suspend domains. Several have no formal policy, according to FoI requests we have made. Some of the agencies, such as National Trading Standards, a private company, are not subject to the Freedom of Information Act 2000, and others including the National Crime Agency, are exempt from FoI.

In other countries, such as Denmark or the USA, a legal process is required before domains are suspended or seized.

With each of these cases – CTIRU, PIPCU's Infringing Website List, and Nominet domain suspensions – the UK has established no real accountability, oversight or independent appeals processes, despite the potential impacts on free expression, the right to property and to run a business. While the number of errors may be small, they will exist, not least because of the scale of the takedowns and removals.

[1033] https://wiki.openrightsgroup.org/wiki/Nominet

3c. What processes should be implemented for individuals who wish to reverse decisions to filter or block content? Who should be responsible for overseeing this?

Ideally, platforms would put in place processes which mean individuals are able to challenge decisions to filter or block their content.

On online platforms, existing processes of content removal generally include three parties: the platform, the user as originator of the content, and a third actor who wishes for the content to be removed. Currently, many of the existing processes are not designed to consider all three users fairly and do not give enough weight to the platform user as the originator of content.

All sides of a dispute need to have the ability to assert their rights or raise the dispute in court. It is unfair for anyone to be unable to raise their side of an issue in a court of public opinion.

In answering this question, the first thing to determine is who is asking for a decision to filter or block, and why. Different reasons require different processes. Copyright is very different to harassment, defamation, or terrorist content, for example.

Content removal from platforms is largely a contractual matter, and the difference in bargaining power between the platform and the user is massive. In practice, the only party who can interpret the contract is the platform. If somebody objects to their content being removed, the only practical recourse is to embarrass the platform into changing and restoring it.

One visible example of this was Facebook's removal of the Pulitzer Prize winning image "The Terror of War", depicting a young girl burned by napalm during the Vietnam War. Facebook removed the image initially to comply with its rules on nudity, and the image was only restored to the platform after significant media coverage was generated surrounding the removal. Recently, a "Volunteer Army" of content creators have also been forced to assist with appeals to YouTube on behalf of content uploaders who have had their content removed from the platform without access to appeal.[1034]

Similarly, in 2013, ORG worked with a Turkish digital rights group - the *Alternative Informatics Association* (AIA) - who were representing activists who had been operating a Facebook page, *Ötekilerin Postasi*, which was removed without warning. ORG and AIA worked to arrange a conference call with Facebook in Ireland to allow the page's administrators to appeal for their content to be restored.

[1034] https://motherboard.vice.com/en_us/article/pavyp8/youtube-contributors-trusted-flaggers-feature

Both the Vietnam image example and the example of the Turkish activists highlight an important issue with the moderation approach of online platforms - namely that the "ordinary citizen" is highly unlikely to be able to challenge the removal or moderation of their content unless they can generate significant media exposure, or can involve third party rights groups in the process.

An example we have seen in our work on our *Blocked!* project - which documents websites blocked by ISP-level adult content filters - is that sites can be accidentally blocked without necessarily containing any content that is inappropriate to minors, and site owners may be legitimate businesses and may be unaware of this fact. We built our tool to allow site owners and interested members of the public to directly appeal to the Internet service providers to request the unblocking of particular sites which did not host any adult content.

The above example of the *Blocked!* project perfectly highlights a problematic system in which users who may be affected by content filtering or blocking are not provided adequate knowledge that they may be affected by a decision to block, and are not provided easy avenues of recourse to reverse such decisions.

For this reason, we would like to see independent processes to interpret the meaning or community standards particularly when those platforms are particularly important for the dissemination of information.

4. What role should users play in establishing and maintaining online community standards for content and behaviour?

If users are to be expected to establish and maintain online community standards for content and behaviour, this should vary from platform to platform. Even within platforms, community standards will differ. Large platforms like Facebook cannot reasonably be considered to be a single community. Rather, particularly large platforms can be considered to be sets of smaller communities, each of which may have their own individual standards.

Some platforms already allow in their design for users to maintain and establish community standards. Facebook and Reddit make clear attempts to devolve moderation and ownership to people controlling pages and groups.

It must be recognised in response to this question that *legal* standards for content are very different to standards for behaviour. Additionally, posts which are individually lawful may become unlawful or otherwise unacceptable as part of a pattern of behaviour.

Often, we find that users are not best-place to establish community standards. Users tend to exhibit a 'mob mentality' and opt to remove content which is lawful, rather than focusing on ensuring that policy or fundamental rights questions such as freedom of expression are at the forefront of their consideration.

5. What measures should online platforms adopt to ensure online safety and the protection of community values or standards, while also protecting the rights of freedom of expression and freedom of information?

It should be noted that criminal law applies online as well as offline. Criminal behaviour should not be tolerated. Criminals should be prosecuted. Measures of disruption are problematic because they evade the prosecution of criminals, and the rights of redress and due process.

Platforms can and do take measures to reduce the occurence of unwanted behaviour. The main issue for policy makers is that much of this behaviour is unpleasant but legal. Trolling – in the traditional sense of deliberately provoking unpleasant arguments – is hardly illegal. Bullying behaviour does eventually become harassment and intimidation, but a certain threshold has to be reached.

Modifications to platforms can and should be made to devolve moderation, report and flag abuse, and to incentivise good behaviour. However, the corollary of *reach* and *availability* is that *gaming* and *abuse* are potential factors, whether it is the familiar email spam and fraud, or groups of immature individuals attempting to provoke or bully people they do not like. While platforms must try to reduce these behaviours, not least so their products do not become poisonous and unpleasant to use, it may be hard to eliminate them entirely.

Given that platforms do have incentives for good behaviour and customer experience, it is somewhat surprising that these have become apparently very serious issues for some users. Similarly, the rights of users to participate and exercise their right of free expression should not be overlooked.

Platforms are attempting to find technical solutions through pattern recognition (machine learning, or "artificial intelligence") to reduce unwanted behaviour. This has its place, but also contains risks of mis-identification, particularly of behaviours like anonymity, incomplete personal details, use of privacy technologies or sporadic posting, as equating with bad posting. Platforms take it upon themselves to be the sole interpreter of their contracts, except when facing publicity storms. In short, there is the potential for reasonable content and behaviour to be mis-identified.

We must also recognise that there is no right to avoid offence. Sometimes free expression depends on the ability to offend. Without the right to offend, there would have been no enlightenment, no Galileo, and no science. Technologies must avoid equating controversy with poor behaviour.

The further question is whether there are interventions governments can or should make. So far we have not heard suggestions that seem proportionate and effective, without creating serious harms to free expression.

6a. What information should online platforms provide to users about the use of their personal data? How should it be presented?

The GDPR is the key starting point here. There are several concrete prescriptions for information that must be presented when collecting data from individuals, what is collected and for what purposes, etc.

There are some good example of how and when to provide information. Context specific reminders are particularly effective.
There is one area where the situation is less clear. GDPR mandates companies to provide information on automated decision making and profiling in an attempt to stop the growth of a black box society, where individuals are at the mercy of opaque computer systems.

This information has been described as the right to an explanation, but its scope is unclear. In addition, modern machine learning systems defy explanations in the conventional sense. We simply cannot explain why the computer has made a decision.

6b. Does the GDPR, in your view, provide sufficient protection for individuals in terms of transparency in the collection and use of personal data or do we need further regulation?

GDPR sets a baseline for data protection, but is not a solution for all sets of privacy risk. Some classes of data arguably demand stronger protection than the level provided by GDPR. In these scenarios, specific additional frameworks can be put in place to protect the data. An example of this is the *PCI DSS* standard, which is an information security standard which defines additional measures that need to be taken to secure payment card information.

At this point, we would also highlight the importance of addressing the lack of consideration of privacy in the proposed system of age verification for pornographic websites, as found in the Digital Economy Act 2017. Age verification requires all visitors to pornographic sites to take steps to actively prove they are above the age of 18. It is arguable that age verification data, which is capable of linking users' ID documents to the pornographic content which they visit, requires an even greater standard of protection than even payment data. There is currently no standard beyond data protection law for the protection of this data. We would strongly encourage the creation of a separate *PCI DSS*-style standard for the protection of age verification data.

7a. Is competition law effective in regulating the activities of these platforms?

Caution should be exercised when trying to use competition law to regulate the activities of online platforms. Platforms do not fit into the remit of competition law easily, as they are not abusing monopoly power in financial terms. There is no 'social media monopoly' that can be identified using competition law.

Additionally, actions under competition law are likely to need to be brought within the jurisdiction of the United States, as this is where the majority of large online platforms are based. The United States has shown little willingness to engage with the idea of breaking up large online platforms.
Furthermore, the idea of 'breaking up' a large online platform such as Facebook is difficult to implement practically. It is unlikely that it would be practically feasible to break up a platform like Facebook into a set of smaller entities which each took on some of the functions of the original platform.

In the digital world, people seem to have a preference for a 'single solution', whether that be open protocols like Email or the Internet Protocol, or centralised platforms such as Facebook. Thus, rather than attempt to break up platforms which appear to have a monopoly on services of their type, it may be more worthwhile to focus on creating open and interoperable standards. It is, however, difficult to know where to intervene to achieve that desired effect. Perhaps platforms could be forced to maintain a greater degree of interoperability and permeability - for example, so that people outside of Facebook can contact people using Facebook.

8. What effect will the United Kingdom leaving the European Union have on the regulation of the Internet?

One specific issue to be highlighted is the potential loss of the protections of Article 15 of the Electronic Commerce Directive after leaving the European Union. Please find enclosed along with this document a separate submission from us which highlights the critical importance of taking action to preserve Article 15 after Brexit takes place.[1035]

In addition, we have concerns that the DCMS and other Governmental departments may not have the necessary resources to cope with the reality of ensuring that all of the appropriate EU Directives and Regulations are incorporated into the UK regulatory framework after leaving the European Union. To highlight this point, GDPR faced over 3,000 amendments, and the recent Telecoms Package is facing similarly high numbers.

In the UK, the House of Lords acts as the scrutiny vehicle for legislation, but is not resourced with large staff research teams. Similarly, the Commons is not set up for line-by-line scrutiny and amendments of complex technical legislation which requires consideration of matters that are not yet in the public eye.

The temptation here will thus be for the Government to adapt and water down future EU legislation. The good but controversial parts such as consumer protections, strong regulatory powers, or commercial obligations are likely to be left out.

[1035] See: Appendix B: *Article 15 ECD Submission.*

9. What should be the function of international organisations in the regulation of the Internet? If so, what should be the role of the United Kingdom in these international organisations?

Here there is a difference between content, telecommunications infrastructure and the Internet. All of these could be improved, but there is no silver bullet.

Telecommunications

The International Telecommunications Union regulates the basic infrastructure of cables and electromagnetic spectrum. Here governments have a big role to play and the UK could do a lot to ensure more democratic participation from civil society.

The EU plays a big role in standards because it can mandate some of these in their technical regulations through European Standards Organisations. Many of these EU standards become international standards. After Brexit, the UK situation will change. The British Standards Institute (BSI) is pushing to retain full membership of ESOs. This may be possible, but the link to EU policy will likely be lost.

Internet

The technical details of the Internet proper are mainly decided at standards bodies such as there Internet Engineering Task Force and W3C, and some key governance institutions such as ICANN.

Governments - other than the US Government - are less influential in these spaces. The Internet Governance Forum is a UN-supported body that is meant to bridge this gap, but it is fair to say that it is not very effective.

The UK has tried several times to start its own processes of international governance, such as the Seoul cyber summit, but these have not worked. It would be better for the UK to spend its energies improving the governance of existing spaces.

Content

Content regulation mainly works at national level, with some important influence from large geopolitical entities. The situation could be summarised in that the EU is setting the standards for privacy, and the US is for most content rules.

Other important elements of the landscape are the OECD recommendations on various issues, and the Council of Europe conventions, e.g. on data. For the UK the latter will be particularly important after Brexit.

May 2018

Open Rights Group – oral evidence (QQ 21-27)

Tuesday 1 May 2018

Watch the meeting

Members present: Lord Gilbert of Panteg (Chairman); Baroness Bertin; Baroness Bonham-Carter of Yarnbury; The Lord Bishop of Chelmsford; Viscount Colville of Culross; Lord Goodlad; Lord Gordon of Strathblane; Baroness Kidron; Baroness McIntosh of Hudnall.

Evidence Session No. 3 Heard in Public Questions 21 - 27

Examination of witnesses

Myles Jackman, Legal Director, Open Rights Group; Javier Ruiz Diaz, Policy Director, Open Rights Group.

Q21 **The Chairman:** I am very pleased to welcome the second set of witnesses to our inquiry this afternoon. I remind you that the meeting is being broadcast online and a transcript is being taken.

We are asking whether a new and comprehensive strategic regulatory framework is or is not required for the internet. Our witnesses come from the Open Rights Group, a think tank that promotes freedom of speech and data protection. Would you introduce yourselves and, so that we get a sense of where you are coming from, tell us whether you think there is a need for a new regulatory framework; and, if so, the form it should take? Should it be self-regulation, co-regulation or more direct regulation?

Myles Jackman: I am the legal director of the Open Rights Group, which, as you have heard, is predominantly a digital rights campaign with particular emphasis on privacy, data protection and free speech issues.

I am a solicitor advocate. I have a private practice—Hodge Jones & Allen LLP—and specialise in what I call obscenity law as a niche practice. As a practitioner, my area is almost exclusively criminal. I practised 10 years PQ and 18 years in the criminal justice system, but my interests today are clearly about freedom of expression.

Before answering the first question, one thing I would like to flag is the regulatory gaps that are already occurring with regard to age verification under the BBFC, which was supposed to come in at the beginning of last month. We see a gap between the BBFC's remit to oversee age verification and the ICO's ability to rectify problems with regard to mistakes or data loss and leaks, which perhaps I may be able to go into later. In this country, between 20 million and 25 million adults are likely to sign up to age verification in the first month. If data on age verification through various service providers is lost, breached or hacked, we are in a very dangerous situation which I suggest GDPR is insufficient to rectify. In the Ashley Madison hack, people committed suicide. For 20 million to 25 million adults in this country, it is a very serious concern. If legislation were considered in that area, we would be very supportive of it.

The other point I would like to make very swiftly is about necessity. Any form of regulation should be necessary and proportionate to the stated aims and perceived harms. I think we are in agreement that we are looking towards the lighter touch-end of co-regulation. Self-regulation may create problems of recourse for users, and the heavier end of the spectrum may be far too difficult for freedom of expression.

Javier Ruiz Diaz: I am the policy director for the Open Rights Group. We work on the internet as a whole. We are not just a privacy organisation or a freedom of speech organisation. We try to represent a grass-roots membership. More than 50% of our support comes from individual donations. We do not claim to represent every internet user, but we think we provide a grass-roots perspective, combined with a high level of expertise. Many of our supporters are people you will find giving evidence to this Committee, such as software engineers, and many are at the top of companies. We try to balance perspectives.

On the regulatory framework, we do not think we should provide a completely new framework for the internet as a whole, first because the internet is too complex for one regulation. We sometimes conflate large platforms with the internet itself, which is simply a shared protocol for the interconnection of various private networks. When we talk about internet regulation, it probably needs to be a lot narrower. Secondly, right now clearly the driver is internet platforms, so we should probably focus on regulating them.

On the second question, we need to protect the open internet. Over the past two years, we have been hearing all sorts of proposals from the UK, the EU and the US for restrictions on content. We do not want to romanticise too much a mythical open internet that has never fully existed. We do not want to say that there are no problems, but at the same time we do not want to throw the baby out with the bathwater. We should recognise that the level of interoperability brought about particularly by the removal of liability in certain conditions, and the removal of the obligation for monitoring content from providers, has worked quite well in many contexts, although we can see limits.

Thirdly, on the question of online and offline, which was mentioned in the previous session, in the main, we take the position that we should have the same principles both online and offline. We need to be very understanding of how technology will shape the implementation of those principles. It is equally wrong to demand that something that works offline works exactly the same online—because it will not—as it is to say that the online world should create completely new rules. For us, things such as due process and respect for human rights should operate across the board.

Finally, there is an important point, which was made before, about the role of private actors. The internet is nothing but the interconnection of lots of privately run infrastructures in the main, with exceptions in certain countries where states still have responsibility for telecommunications. When private actors are intermediaries, anything that gets enforced, whether it is public policy or the demands of other private actors, will have to go through another private actor. That means that companies have to make legal decisions potentially as to the application of human rights and balancing freedom of expression. It also means that the obligations of states to uphold fundamental rights can be weakened, because if a Government decide to censor a bit of content directly, they will have to apply human rights very clearly. If a Government nudge a private company to implement some form of content restriction, many people would argue that companies do not have the same responsibilities.

We would argue that private actors have some responsibilities, particularly providing a foreseeable environment for users. When Governments mandate restrictions, they should be a lot more up front about what they do, and should not try to corral internet companies into a room and threaten them with regulation or else, unless they do something. That is the worst of both worlds and it lowers the level of accountability.

Q22 **Baroness Kidron:** I want to ask you about what you have just said, to make sure that I understand it completely. It feels as though there is a bit of tension between one set of private actors, another set of private actors, the open internet and the intermediary platforms, about which I am about to ask you. My question, which I know you heard earlier, is about whether platforms are publishers or mere conduits, or do we have to think of them in a different way? In answering that question, could you also unravel whether you think there is too much power in some of the bigger private actors against the little ones, who might be the users, who are not represented by the Government in the way you set it out?

Javier Ruiz Diaz: It is absolutely clear that the concentration of power in a handful of mainly US companies has brought bad consequences across the board. As the previous panel said, it is a lot harder to know how to deal with it. One of the things we are concerned about is when we see removals, or it is said that we should deal with it through the removal of liability. That will affect the internet as a whole.

The North American view is that hosting protections do not apply to organisations as such. A platform is defined in the European context as a two-sided market, so there are users, who are like consumers, and there are advertisers, or people trying to sell or buy cars, and the platform is in the middle. Platform is the modern way of describing those organisations. I do not know whether there is any more modern term that we can use to describe them.

The fundamental point is that the liability protections do not attach to the organisation; they attach to individual bits of content and activity. If a newspaper is running an online discussion forum, some liability protections would be attached to the content produced by people commenting. Conversely, if a platform, such as Netflix, attaches its own content, at that point it will clearly stop being a host and will start becoming potentially a publisher, or something else. It is very important not to try to categorise platforms as a whole either as publishers or not. Protections are attached to specific activities, so we need to break down the activities and try to focus on each specifically.

The Chairman: Do you want to add anything, Mr Jackman?

Myles Jackman: I have nothing to add to that, because we prepared alternate questions. Forgive us.

Baroness Kidron: Well done. Can I ask the same question about design? We tend to concentrate on content, but the design of some of the interlocutors has a profound effect on the experience and behaviour of users, so I am interested in your perspective on the freedom of the user and how you deal with that tension.

Javier Ruiz Diaz: Design is obviously very important. One caveat in this context is that the design of a platform such as Facebook or Google is not like the design of a simple product. These platforms are running A/B testing all the time. There is a high probability that the results you get from your search will not be the same as the ones you got yesterday, or the ones that the next person will get. It is not that they are designed by committee, but there is no mastermind designing everything all the time. Apple and other companies may be a bit more centralised, but it can be quite hard to have a clear central vision of the design for such a large, complex system.

Baroness Kidron: Let me put the question another way and ask about the culture and principles of design.

Javier Ruiz Diaz: We are running a European-funded project on ethics in design. With various universities, we are looking specifically at that question, mainly in the context of internet of things products, which are a lot more manageable than designing Facebook or Google. Our approach is that you cannot have ethics as a single step where you say, “We are going to pass the ethics hurdle”, or, “We are going to have an ethical accord and do some rubber-stamping”. You need to embed ethics in day-to-day organisation, and try to become ethical and strive for excellence in everything you do.

A whole new branch of ethics and technology is now trying to move in that direction, rather than simply providing a checklist that the organisation will comply with, or simple processes that everyone can go through. That can be satisfactory, in the sense of making you feel good that you are ethical, but we believe that you need to become ethical; it has to be an ongoing process, and that is a lot harder.

Baroness Kidron: Can you answer this with yes or no, because I am running out of time? Do you believe that that ethical structure has to sit outside a regulatory structure? Once we have decided what they look like, who holds the ethics?

Javier Ruiz Diaz: We definitely would not want to see ethics in any form completely superseding regulation. What we hear from industry lobbies is, "Please don't regulate us; let us run our own ethics". There are ethics inside regulation and space for ethics outside, but there should definitely not be a substitution. It would be quite difficult to have any kind of official body mandating ethics as such. There are ethical committees at universities, for example. You can have specific interventions, and trying to create anything that involves rubber-stamping or a certificate can work, but it should be a process rather than a simple step.

Q23 **Viscount Colville of Culross:** You heard the previous witnesses refer to the need for platforms to have more responsibility for the way they host and moderate content, so that they are fairer and more transparent. What is your view on that? Mr Diaz, from the other side, you said we do not want the regulators locking internet companies into a darkened room and threatening them. Do you think that the processes being used at the moment by law enforcement agencies and other bodies, such as the Internet Watch Foundation, are working? Are they fair and transparent enough, and what else could be done to make them work better?

Myles Jackman: Those are questions I have prepared. With regard to the first part of the question about processes, accountability and fairness, we have significant concerns that they do not appear transparent, fair and accountable. It may be an appearance, but for fairly obvious reasons, these platforms require swift action, and moderation has to be light touch in those terms.

Our concerns are that it almost becomes a proxy for right and wrong. Perhaps I could use the example of nipples on Facebook. If you are not aware of it, I am sorry I have to go into this. Fourteen is the standard age for Facebook, but for adults over the age of 18 male nipples are perfectly acceptable; female nipples are verboten; and Facebook is very confused about trans-nipples during transition. My point is that containing nipples almost becomes a proxy for adult content when it is not, if you see what I mean.

The next point is that there is essentially a contractual issue where the people who want to seek redress are not getting it directly from the platform in question. A good example of that is the Vietnamese girl napalm photograph that was initially only brought to public attention through the press. If you have traction, you can get redress, but the problem is that it is virtually of no precedent value whatsoever; in other words, unless we are talking about that picture of the Vietnamese napalm girl, in which case there is a judgment, it does not apply across the spectrum.

We also have concerns about tone, context and nuance. Anyone who is attempting to moderate should be able to identify sarcasm and irony, which clearly will be problematic, at this time, for algorithms, but we appreciate that platforms operating at speed must have some level of hard and fast rules. We do not know enough about how their systems work and operate, what criteria they use, who has specifically decided the criteria and who arbitrates in a borderline case, such as the image of the Vietnamese girl.

If I may move on to law enforcement, from an obscenity law perspective I was thinking predominantly about what I call proactive police law enforcement and reactive police law enforcement, among the other forms it takes. Earlier reference was made to indecent images of children, which I assume we all agree should have no place, but, tragically, sites, including Facebook, are capable of hosting that material.

As you may be aware, hash values in metadata should be able to track those images, so, if someone were foolish enough to upload such an image to Facebook in any capacity and in any form, it should be identified. Under the Protection of Children Act 1978, in this country there is clearly some form of law enforcement effectiveness. It becomes less effective with slightly lower-level offences, such as the extreme pornography offence under the Criminal Justice and Immigration Act or Obscene Publications Act offences and so on. The material might be adult, and arguably consensual, but it is only reported to police; it is not proactively sought.

The problem areas we find are the Counter Terrorism Internet Referral Unit, CTIRU, and the Police Intellectual Property Crime Unit, PIPCU. They have some very specific issues we have rubbed up against and not found satisfactory answers to. Data about CTIRU's operation are so scarce to us that it is impossible to assess its systems, to see how accountable and transparent they are. Based on that, we would have to come to the conclusion that they are certainly not transparent. There is accountability within the police, but it is difficult to assess to what extent it is evaluated and effective outcomes are either agreed or disagreed on, and for fairness, in the criminal justice sense of fairness, that cannot be true.

The other thing is PIPCU's infringing websites list that it shares with advertisers to stop piracy online. The list is secret. Police say that they do not force advertisers to do anything, but the restriction on freedom that suggests is that the advertisers are contacted and feel that they must respond to those inquiries.

The IWF, which I think was the formal part of the question, is arguably more transparent, but none the less accountability becomes complicated.

There is an Article 10 issue at play there, I think. I hope I have addressed some of the points as swiftly as possible.

Viscount Colville of Culross: Do you think more could be done? We heard last week about problems with the take-down regime; it is not standardised enough and it is not clear enough how it should work and where responsibility should lie. Do you think more could be done to develop that?

Myles Jackman: For the purposes of clarity, if we are talking not about indecent material but about normal material, shall we say, absolutely, yes. There should be a notice and counter-notice process whereby the user can challenge and is notified. If I might extrapolate, I suggest that it should go as far as blocking orders. If something is blocked, I should know it has been blocked, particularly if it is my site, as happened under the adult filter; my obscenity lawyer site was temporarily filtered out. Other people told me that. My point is that you do not know you have been filtered out, which is particularly problematic if you are a business owner and do not realise why you are not getting business. Clearly, notice and counternotice are very necessary. Another point that should be given very serious consideration is right to appeal.

Viscount Colville of Culross: How might that right to appeal work? What form would it take?

Myles Jackman: We are talking in such broad terms that it is difficult.

Viscount Colville of Culross: Not obscenity.

Myles Jackman: It would not be in an obscenity motion, because clearly there is a pre-existing criminal framework for that. What I am talking about is blocking for other purposes—for example, PIPCU and intellectual property infringement material. There should be a notice on sites such as that, and manufacturers and the site owner should be able to challenge it. That is where the appeal process should come into play. At the moment, we have very little idea how that operates substantively.

Baroness Kidron: You came out shooting, saying there should be no regulation, but, if you have a right of appeal and all these processes, where does it all sit?

Myles Jackman: I thought I said that we wanted light-touch co-regulation.

Baroness Kidron: That would include universal standards, take-down standards and that sort of thing.

Myles Jackman: Absolutely.

Javier Ruiz Diaz: It could even go further. Content that may be illegal could arise in many contexts. Going through the courts eventually would be the preferred course of action, but a lot of content is dealt with under terms and conditions, as was mentioned. There is a question as to whether content should be dealt with by terms and conditions when you are dealing with illegality, which is fundamental for CTIRU, where they use terms and conditions to take down material of a terrorist nature or of use to terrorists.

If we restrict ourselves to terms and conditions, there is an issue right now in that companies' internal processes are even worse than anything we have heard before from CTIRU. There is absolutely no transparency. We had to mediate between Turkish Facebook users when the main protest website for the equivalent of the Arab spring, the Gezi Park protests, was taken down by Facebook. They had no recourse. We were contacted by Turkish activists. We went through to Facebook in Ireland and organised a conference call so that Turkish activists could talk to Facebook. Clearly, that is not satisfactory. There is a huge gap.

We need much stronger due process for internal take-downs in companies. At some point, we think it would be worth exploring some form of arbitration, in the same way that if I disagree with my plumber I can go to an arbitration body. We do not want in any way to weaken the rule of law. Our position on that is clear; it is not to say that website take-downs should not go through the courts, but when it comes to decisions based purely on the terms and conditions of social media platforms internally, it would be an improvement in the current situation to have some form of external arbitration.

The Chairman: Your external arbitration would be in the co-regulatory framework that you are advocating.

Javier Ruiz Diaz: It could be part of a co-regulatory framework, although in this case it could even fall below the regulatory framework. We would want it to be stronger, with as many teeth as possible, but it would be an arbitrator, not a full court. Obviously, you should always be able to go to court. In theory, you always can go to court within the limitations of costs and actual opportunity.

We looked at oversight. At the moment, we mainly know about content take-downs by companies from the reporting of those companies. Such reports tend to be at international level, so Google in the US would do it internationally. They may give a bit more detail, but we think there is a need for more oversight, possibly even within countries, to try to understand how companies themselves take down material. In particular, we find huge discrepancy between the many thousands of items that CTIRU claims it takes down per year, and the very few in internet companies' own reports, so there is a need to tally those figures.

Q24 **Lord Gordon of Strathblane:** The Government's digital charter states that one of the key guiding principles is that people should understand the rules that apply to them when they are online, yet earlier this afternoon a witness quoted alarmingly high statistics of people who simply did not know. How do we remedy that?

Myles Jackman: It does not have to be through a regulatory regime per se; in other words, tragically, we are suggesting that age verifications cannot perform. People will only learn the importance of digital privacy afterwards.

Lord Gordon of Strathblane: When it is too late.

Myles Jackman: Absolutely. To develop that point briefly, that is why we suggest that, in the limited circumstances of higher-level intrusive private data, GDPR is not quite sufficient. If there are between 20 million and 25 million adults whose information can be hacked fairly easily, we are probably looking at many tragic suicides and people feeling ostracised from communities—everything you would not want to happen from the internet. I hope we can avoid that. I can certainly see a basic information or leaflet-type website to understand your rights, particularly under GDPR, as it is so current and a lot of people are working on it; but if you are not a data controller you might not even consider the issue, so I entirely agree that it is difficult to educate and enlighten people as to their rights.

Lord Gordon of Strathblane: As someone who recently downloaded new terms and conditions on my app, I find it difficult enough to make my fingers small enough to press the right button, let alone read the contents. Surely, there is a way round this. Terms and conditions could be verified by an external body; I do not want to use the word "regulator" because it gets you quite excited. It could provide a kitemark indicating that the terms and conditions are reasonable. For all I know, I could be signing away my house to Facebook or Google.

Myles Jackman: Sadly, that is quite a common experience. I agree. I find it very difficult, even as a lawyer, to go through those terms and conditions. Jurisprudence coming out of the commercial courts and so on is increasingly towards comprehensible terms and conditions.

Lord Gordon of Strathblane: How do we do it?

Myles Jackman: Short, brief points. I agree with your broad proposition about an independent body arbitrating terms and conditions, particularly privacy policies, with the ability to understand that a privacy policy may be changed at a later date, to use age verification as an example. There is an opportunity for regulatory capture for an actor; MindGeek is the owner of approximately 90% of the adult tube sites on the internet, and it could simply capture the British market of adult content consumers, or even globally, and then change its privacy policy six months or a year down the line, as Facebook has continued to do, by adding widgets and so on.

Lord Gordon of Strathblane: But surely there should be somebody stopping them changing their policy like that.

Myles Jackman: That was an example I was using to substantiate the point. Forgive me if it did not come across as clearly as I hoped.

The Chairman: You advocate co-regulation. You think somebody should be doing these regulatory things. What do you mean by co-regulation?

Javier Ruiz Diaz: When it comes to information around privacy, we already have a very clear regulatory framework with the Information Commissioner. When we were here a few months ago talking to a Committee about artificial intelligence, there was a big discussion as to the role of different regulatory bodies. In general, our approach would be to make the most of the bodies we already have before we start building new ones. That would be our general principle.

It is important to understand the difference between terms and conditions in establishing some form of contractual relationship, and saying that now other relationships are ruled through that contract. We believe that in most cases it would be a one-sided contract, probably not fair and possibly unenforceable. There is a difference between that and the previous policy, which is highly regulated under Article 13 of the general data protection regulation.

Lord Gordon of Strathblane: I am not a lawyer, but you said it would be a one-sided contract, probably not fair and unenforceable. Why would it be unenforceable?

Javier Ruiz Diaz: If both sides cannot agree, it could be hard to enforce.

Lord Gordon of Strathblane: But if I have signed a contract with somebody, surely it is enforceable. I speak as a layman.

Myles Jackman: Might I suggest that there is arguably an imparity of bargaining power between an enormous corporation such as Facebook and individuals such as ourselves? It has been suggested that withdrawal from a platform means that other platforms may take up the slack, but ultimately your choice may be either to be able to engage or not. There will be people for whom Facebook simply is the internet. In short, it is their portal, their gateway; that is how they understand information on the internet. That concerns us somewhat and it needs to be remedied.

Javier Ruiz Diaz: The important thing to understand is that certain things are regulated under data protection. Terms and conditions can be a very broad range of things. It could be how companies use your information, or assignment of intellectual property could be an issue. Use of data is fairly well defined in the GDPR, so companies need to start sticking to the letter of GDPR as much as possible.

Lord Gordon of Strathblane: You think that bit of the GDPR is adequate.

Javier Ruiz Diaz: In providing a baseline, yes. Articles 13 and 14 of GDPR give a baseline for the information that should be provided. Obviously, we think it is not enough.

Baroness Kidron: I want to pick up your point about the split. Do you think there might be a role for consumer law around terms and conditions rather than data law? The GDPR was developed in a period when we thought of consent as the key factor, but in the world of smart cities, smart cars, smart fridges and smart everything, the idea of consent is somewhat redundant, because we just walk through it all. You might be very good people to tell us something about that on the record.

Javier Ruiz Diaz: In one of his last bits of work, the outgoing European Data Protection Supervisor, Peter Hustings, defined a framework for the regulation of big data. He proposed that data protection, consumer regulation and competition should work in unison, mainly because there were issues about consent and even about whether some data is identifiable enough to be protected under data protection.

We think there is a huge role for consumers. We have campaigned for full implementation in the Data Protection Bill of Article 80(2) of GDPR, which would give consumer organisations, such as the Open Rights Group, power to take independent action without the need to be instructed. We are also pushing for stronger class action powers. It is not just the idea of consumer action; we need the crafting of consumer protection itself to complement regulation and accountability.

On consent, most privacy advocates nowadays are moving a bit away from consent, mainly because in the US it is constructed as a way to get people to part with their information and to gather data. Most people now say they want to see systems where data is minimised, which is another principle in law. In particular, we want to see in law that consent should be attached to meaningful, real choices. If you do not have a choice to part with your data, you should refuse consent. That is the way it should work, but it is not always the way it actually works.

For example, right now if you use Facebook, you get a big pop-up that will drive you through certain questions. The way the dialogue is constructed nudges you towards agreeing with everything it says there. Somewhere else in the terms and conditions, Facebook says that its use of your data is in order to provide you with a service, which is more or less a contractual relationship. In that context, you do not have a choice; consent is removed. The real level of consent Facebook gives you is very unclear.

Baroness Bertin: Can I bring you back to the point about balance and ethics? I hear what you are saying about an open and free internet, but clearly there have been some unintended consequences, and no one would disagree with that. Will we ever find a resting place on that? We heard recently from the Metropolitan Police Commissioner that social media—Twitter—were leading directly in some cases to gang murders. Is that a consequence of an open internet, or should something be done about such things?

Javier Ruiz Diaz: We should really focus on the problems as narrowly as possible. The statement that Twitter has led to a murder is very broad, and it is quite important to see how exactly the use of Twitter contributed, and what elements were Twitter as Twitter, and not—

Baroness Bertin: They are not allowed to cool off; they go crackers online and suddenly it has fallen out into the streets and ended in a knifing. Presumably, that is why she said that.

Javier Ruiz Diaz: In that context, it is important to understand what could have been done differently. What is specific about that particular platform compared with an argument in a pub that escalates into violence? We understand that there are issues around the internet, and what was said in the previous session around the removal of inhibitions.

Baroness Bertin: That is a key point, is it not?

Javier Ruiz Diaz: It is critical. There is quite a lot of research. We are not experts on online communications and the psychological effects. Clearly, we can see that the level of abuse, particularly of women, on Twitter is unacceptable. What features of Twitter would you change? Then it becomes a matter of design. It is quite a complex question and it is hard to solve with a simple silver bullet. In order to deal with such questions, which are completely legitimate, I am afraid you need to get into the detail.

Baroness Bertin: We have talked about ethics, design and all the rest of it. Are ethics going to win over profits?

Lord Gordon of Strathblane: There is always a first.

Javier Ruiz Diaz: The ethics would have to stretch beyond the data aspects and into wider corporate issues. In the US, there was a big drive to introduce ethics in the corporate world after the Enron scandal. Unfortunately, it seems that it has mainly generated a whole industry of ethics advisories for large corporations rather than real ethical change. I agree that it is a fundamental, large problem.

Q25 **Baroness Bonham-Carter of Yarnbury:** I want to pick up on what Lord Gordon mentioned earlier: people's lack of awareness as to what can happen to them when they use the internet. A report by Doteveryone showed that 83% of those surveyed were unaware that information can be collected about them. What information should online platforms provide to users?

By the way, I wish the Bishop had come in with his brilliant question about the definition of a platform, but we do not have time to go into that. I hope you heard his question in the earlier session about the use of personal data and how it should be presented. Picking up on something slightly tangential, which we were talking about last week, how about the misuse of a person's reputation falsely to sell things online? That is a slightly different question, but I wanted to get them both in because we do not have much time.

Javier Ruiz Diaz: As I said before, GDPR is the baseline for the information that should be provided, and that particular aspect is fairly prescriptive. There are a couple of issues. One raised earlier was about rights relating to data portability. It is not specifically about information, but more about the wider framework.

Companies will now let you download your data from their websites. You can go to Google or Facebook and download a lot of the information they have, not everything but quite a lot. The problem is that you cannot do much with it, so there are questions about interoperability and getting companies to accept data and find common formats. That will be important. It will be really challenging for Facebook, because it is very complex, with sections such as news and chat.

Another problematic issue is the use of the information, particularly around automated decision-making, profiling or algorithms where it can be quite a challenge to explain what is being done. It is fairly easy for companies to tell you, "We collect this data and we generally use it for marketing". When it comes to explaining how they will provide it to serve your particular app, we think they should strive for maximum transparency, but we should be aware that there are substantial challenges in making that practical.

Baroness Bonham-Carter of Yarnbury: You accept that it is complicated and that there are challenges, but, to pick up what the Chairman said, what is the resolution?

Javier Ruiz Diaz: Purely on information, we ran a project to look at privacy policies and information rights under GDPR. I am afraid that the solution is to keep up the pressure. It will be quite iterative. If someone raises the bar and other companies develop best practice, we should try to get other companies to follow suit. In this case, we need bottom-up pressure, so we need citizens to be better informed, a stronger civil society able to put more pressure on companies, and regulators to be more involved and take action against companies. There is no simple solution. You have to come at it from all those different places.

The Chairman: Mr Jackman, do you want to deal with the second part of the question?

Myles Jackman: I do not want to put words into your mouth, but what I heard was that we need a specific offence for that type of activity. Was that what you were getting at?

Baroness Bonham-Carter of Yarnbury: No. There is something we cannot mention specifically, but it is very much about somebody's reputation being misused falsely to sell products.

Myles Jackman: To my mind, the element of falsehood would seem to attract criminal liability almost immediately.

Baroness Bonham-Carter of Yarnbury: It does not seem to have helped people who have found themselves in that circumstance.

Myles Jackman: Unfortunately not; I agree, but that is my point about GDPR and the sort of CCTV element of restoration after the fact. I would say that GDPR in the circumstances I have defined is insufficient, simply because it is such a huge intrusion into privacy. Arguably, reputational misuse is equally a privacy intrusion above and beyond mere factual detail. Certainly, I agree with you on the point that it is something that needs to be considered in greater detail.

Q26 **Baroness McIntosh of Hudnall:** You heard the earlier discussion about competition law. The issue is about the scale of these platforms as they have grown over a very short period of time, and the way the current arrangements for regulating competitiveness in any market can or should be applied. Can they be applied, or should something else be developed that can be applied to these platforms? Is there anything about the fact that we are about to exit the European Union that will make us more vulnerable to being at a disadvantage?

Javier Ruiz Diaz: One of the fundamental problems with competition law is that we do not have a good definition of what the market is. Facebook and Google are giants in their advertising market share. There is no social media monopoly category or search. You can see statistics about search, but it is not well defined.

The other problem is that they are not really abusing their power to hike prices. On the contrary, in the short term they give you very good value for money because their services tend to be free. It is quite hard to square short-term benefits with long-term detriments in this context.

The third problem is that the US is the space where competition action should take place, and the US simply has no interest in breaking up these companies because they give their country a huge amount of soft power and influence around the world. It would be against US national interest to break up Facebook or Google at this point. Maybe it will happen at some point in the future, but right now it is unthinkable.

As was said before, competition law is not perfect; it tends to come in after problems have happened, rather than preventing them, and the remedies for individuals can be either non-existent or difficult. They have to go through several hoops to get a benefit at the end.

These companies are technology monopolies. They are created in various forms—for example, intellectual property and rights in the case of Microsoft. There are economies of scale and vendor lock-in. Anyone who has dealt with public procurement on Oracle has horror stories about the vendor lock-in that Oracle imposes on people. There are data silos and network effects; the network effect is one of the most fundamental.

Digital likes simple solutions, and once a simple solution is found, in general, there is a tendency just to use that. We see that in open protocols, such as the actual internet protocol, which itself is an open solution, or email. On the other side, there are closed platforms. There is a choice. If we want a simple single solution, do we want it to be an open protocol that any company can use, or do we want it to be a closed platform? The measures should be aimed at introducing much higher levels of interoperability.

A question was asked earlier about how to break up Facebook. The idea of breaking in the sense of breaking an oil monopoly in the 1930s does not work in the same way for a technology company. You might be able to break up certain subsidiaries and say they cannot buy Instagram or things like that. There is a big question about the merging of databases, and that must definitely be tackled. We did some work with the Transatlantic Consumer Dialogue on that area, and there is some work, mainly in Germany, on data and mergers. When it comes to the natural growth of companies, the main thing to do is to try to promote interoperability and to move as much as possible towards open protocols and avoid platforms.

Lord Goodlad: What do you think the effect will be on regulation of the internet of the United Kingdom leaving the European Union?

Javier Ruiz Diaz: We have one specific question and a general concern. The specific question relates to Article 15 of the e-commerce directive, which more or less forbids the general monitoring of internet content by platforms, hosts or mirror conduits. That article does not transpose the e-commerce regulations. The three previous articles are more or less verbatim, but that article simply disappears. The UK Government have argued that that principle was implicit in UK law in the past.

We see similar things with the IP enforcement directive, which was not implemented either, so there will be a big problem the day after Brexit. The repeal Bill will not incorporate things that are not there, so that is something that should be fixed. If we had to make one concrete recommendation, it would be to bring that into statute before Brexit, or at the time of Brexit; otherwise, there will be divergence in the regulatory frameworks of the UK and Europe. Despite Brexit, the expectation is that, in theory, in the short term things should continue as they are, but clearly they will not.

More generally, we think there will be pressure towards deregulation. We are worried about whether, institutionally, DCMS and Parliament have the capacity to deal with a post-Brexit world. We think it will be quite challenging.

The Chairman: Do you have reason to believe that DCMS has no capacity from your dealings with it, or is it just a general anxiety?

Javier Ruiz Diaz: It is from dealing with DCMS. We do a lot of work for Brussels; we are part of a European network of civil rights organisations.

Looking at the amount of work on legislation and the volume of things coming from Brussels, and thinking about that being translated into a UK position is quite scary. We look at both sides.

To give you an idea, GDPR faced more than 3,000 amendments, and the telecoms package looks something like that. There is simply no way that the UK Parliament can deal with 3,000 amendments. They would not go through. The systems for going through amendments line by line are just not there. People complain about the power of lobbyists in Brussels. To be honest, quite a lot of the lobbying is necessary because it means that external input is taken into account at the time of making laws. It also means that long-term and broader impacts can be taken into account, rather than short-term political considerations, which unfortunately seems to be the case for most legislation in the UK, despite the best efforts of the House of Lords in trying to provide a counterbalance. If we are honest, you do not have the resources that people in the European Parliament have as regards the number of assistants and access to legal expertise. It will be a challenge for the UK to continue legislating at the same level of quality as it has enjoyed until now from Brussels.

Q27 **The Chairman:** I will finish by asking a general question. We have told you the premise of our inquiry, which is to balance freedom of expression with the perceived need to regulate the internet and how we go about it. Could you tell us what freedom of expression means to you, and whether generally in society freedom of expression and freedom of speech is under threat?

Myles Jackman: I was taking notes and I wrote down "perceived need" as part of your question. Forgive me for reiterating that. Freedom of expression is absolutely fundamental to me as an individual. I have reasons for that. As well as being interested in obscenity, as was noted in the *Guardian* a couple of years ago I am a practising BDSMer; I have an interest in alternative sexuality. Therefore, I have a distinct interest in both privacy and freedom of expression and my ability to express my sexuality without imposing on anyone else, or infringing anyone else's consent; so, on a personal level it absolutely resonates with me.

From a historical perspective, I would have said it was the fundamental right on which I view our democracy as being built, if I had to choose one thing in isolation. Reference was made to my coming in all guns blazing, but the fear of regulation is that freedom of expression will be curtailed in different ways. That may be minority sexual communities or it may simply be people's ability to communicate, as we are seeing under the age verification regime. The Lord Bishop of Chelmsford mentioned ATVOD and the AVMS regulations. There was a very small chilling effect under that, in which you might be interested: abuse of regulation. Under ATVOD, there was a duty to investigate, if notification was received of a site not complying with the ODPS regulations.

A dominatrix dropped in about 80 of her competitors, saying that they were not in any way complying with the regulatory regime. What is interesting to me about this in broader terms is that the vast majority of these were one-woman-band private producers, often with children or other dependants, essentially working flexible hours from home. Of those 80 or 90, only two challenged it: UCSC and Pandora Blake—The Urban Chick Supremacy Cell and Dreams of Spanking—and won, and I believe ATVOD is no more because we were successful in that.

That individual shut down about 80 businesses that were absolutely essential to the people who held them. They simply received a notice letter. I hope this is a broader point. Individuals who do not necessarily have recourse to a particularly high level of technical or legal expertise may receive a notice letter and be terrified. All those who shut down their businesses said the same thing: "We've got kids; we have a family life and we need to retain our privacy". That was a clear example of abuse of the regulatory regime for commercial advantage, so I am afraid there is another issue.

The Chairman: That is interesting. You have illustrated, from a personal point of view and from the point of view of your organisation, the importance of freedom of expression. Clearly, any regulation has to be balanced against that. Do you think that in society freedom of speech generally is under threat and not sufficiently respected? Is that a contextual problem in which we are now operating?

Myles Jackman: The internet has given the vast majority of average citizens, who would not have had the opportunity to express themselves and be listened to, a huge freedom beyond their wildest comprehension. If that is restricted in certain ways, and certain communities—not exclusively sexual communities—and individuals feel that it is curtailed, there is the very strong risk of threat to free expression in that regard.

The Chairman: Mr Ruiz Diaz, do you think society takes freedom of expression sufficiently seriously?

Javier Ruiz Diaz: Freedom of expression is one of those things that you do not miss until you lose it. In general, we take it for granted, but we are dealing with a complex interrelationship of various rights. Freedom of expression and privacy are very important, and both are connected. You can add freedom of association. We should not look at human rights in isolation. When we have problems we should try to narrow things down, but we should see how all those different rights play together.

We should not restrict our analysis to a pure rights framework, particularly when it could be seen as some sort of ceiling, whereby as long as you tick the box you have done what you need to. We see it as the flourishing of human life, with people using technology to develop themselves to the fullest. In that sense, human rights are very necessary and they all play together. We should not say, “Have we ticked the box on dealing with freedom of expression?” It is about using those rights to provide a springboard.

Lord Gordon of Strathblane: I do not know whether you are a limited company, or what form of funding you have. Do you produce an annual report and, if so, can you send it to us?

Javier Ruiz Diaz: We will. At the moment, the majority of our funding comes from individual supporters.

Lord Gordon of Strathblane: It is not the funding, but an annual report. Clearly, you operate not just in Britain but in other countries, and it would be interesting to find the scope of that.

The Chairman: If you could send us the report, we would find it a useful piece of information.

Javier Ruiz Diaz: We will, and we are happy to supply any other information.

Baroness Kidron: The freedom that you beautifully described has to be set against, presumably, the freedoms of others, such as the women on Twitter you described earlier. Can I have your agreement to that on the record?

Javier Ruiz Diaz: Of course. The complexity is that it is not just freedom but the value of human life as a whole.

The Chairman: Thank you very much for giving evidence. It has been a very interesting session for us. We are embarking on a very wide-ranging inquiry, and today we have had a wide range of evidence to inform us. Thank you.

Marion Oswald, University of Winchester; Emma Nottingham, University of Winchester; and Helen Ryan, University of Winchester – written evidence (IRN0018)

Written evidence to be found under Emma Nottingham, University of Wincheser

Pact – written evidence (IRN0003)

Introduction

1. Pact is the UK trade association which represents and promotes the commercial interests of independent feature film, television, digital, children's and animation media companies. Pact has presence in production centres around the UK including London and the South East, Glasgow, Belfast, Manchester/Salford, Cardiff and Bristol; with over 500 members; the majority of these are SMEs (small and medium sized enterprises) with a turnover of less than £50m a year.

2. The UK is a world leader in the sales of TV content globally and revenues continue to rise. Taken as a whole, the TV industry around the world is worth $400 billion.[1036] UK independent television sector revenues have grown from £1.3 billion in 2005 to around £2.5 billion in 2017 largely driven by a growth in international sales.[1037]

3. The copyright licensing framework underpins growth in this sector. It enables rights holders to exploit their intellectual property by controlling access to their content which they use to generate revenues to invest in future productions.

4. The UK copyright framework is considered to be one of the best in the world. It has been effective in enabling competition and growth in the television production sector, and as a result:

   - The UK is now the second-largest exporter of television programmes in the world.
   - Audiences in the UK and across the globe have had access to high-quality, thought provoking and entertaining content in a range of different genres, much of which is provided free-of-charge via television broadcasting.
   - The flexibility of the copyright licensing regime has allowed independent producers, including many SMEs, to adapt to changes in market conditions and find new business opportunities in the UK and overseas.

[1036] Analysis for Pact by Oliver & Ohlbaum, published in 'A New Age for UK TV content and a New Role for the BBC', August 2014

[1037] Pact Census Independent Production Sector Financial Census and Survey 2017, by Oliver & Ohlbaum Associates Limited

- There are now many examples of audio-visual content producers working with non-linear digital content providers to create new, innovative content and services for consumers in the UK and elsewhere.

5. Independent producers are using the resulting revenues to become significant investors in the creation of UK content creation and are vital part of the UKs creative industries.

Overview

The TV production sector has benefited from the new technologies that enable the public to access new forms of content. For some years now our members have been able to sell or share their content to new platforms. For example through subscription based video on demand (SVOD) services like Netflix or using ad based business models like YouTube. Platforms willing to pay a high premium for outright ownership of the rights are particularly beneficial to producers because they pay all upfront costs. That said this only applies to a small number of producers. We want to continue providing the best content for these services and there are advantages to us and the wider sector and the UK. Audiences have never had it so good with the amount of choice available to them.

Pacts main concerns about the internet and whether it needs to be regulated is about how to ensure fair remuneration of content. Despite a small number of producers winning lucrative deals with some of the SVOD platforms on the whole the rates that producers receive for other content shown online can be minuscule and inconsistent. Revenues depend on the share of advertising based on clicks per minute. Often payment is not realised because advertisers only pay out revenue to platforms when a viewer watches more than 30 seconds of an advert. How much producers can control access is also important. Working with platforms has been relatively easy to manage access to content and decide how best to develop new business models. But when traditional Public Service Broadcasters (PSBs) also use platforms to distribute content commissioned from our members it has become more complicated. Managing the access to the content is vital if producers want to lengthen the value to any content. That is why we have interests in looking at how to better negotiate better terms with the PSBs when it comes to online content.

Linked to this upholding the current high standards of IP enforcement is important. Pact through the Creative Industries Council has worked hard to get the internet service companies to agree to meet others in the creative sector to discuss online infringement. Through the recently published Creative Sector Deal there is more opportunity to bring forth issues with the internet service providers.

Pact’s response will focus the above key issues below.

Digital rights

- Pact over a number of years has argued the need for reasonable remuneration of digital content. Especially those being commissioned by the PSBs. The PSB compact allows the PSBs to certain benefits, such as access to gifted or reserved spectrum and EPG prominence (and in the case of the BBC and S4C, public funding via the licence fee). Broadcasters are then required to provide a wide range of programmes, and minimum amounts of certain types of programming including UK originations, news and current affairs. The system is based on a compact which balances obligations and benefits. This system no longer exists with digital commissions as normal obligations such as the terms of trade normally agreed with independent producers are forgone. As a result the obligation to invest in a diverse supply of content, which includes investing in a range of suppliers from across the country is diminished.

- The BBC in particular is exacerbating a trend that is happening online when it comes to remunerating content creators. Through BBC3 they are paying minimum rates for short form content which is then shared with millions of users who are not license fee payers. This means producers can not geo-block their content and the subsequent value of their content is lost. As it currently stands the distribution arrangements are only increasing this.

- BBC should acknowledge that indirectly there are competition issues when they decide to unilaterally take the rights of short form content produced by independent producers. For modest budgets producers are expected to deliver short programmes of network quality that the BBC will then give away globally denying producers any chance to try and distribute the content for themselves thus losing out on the revenue, limiting a companies growth and ability to employ more people and invest more in developing new ideas.

- This model is unstainable if these companies are to develop. In spite of the fierce competition in the market Pact wants them to succeed and develop and to grow. This is the next generation of new producers, digital natives who we need to come up with the next big shows or the next international hit that brings in more money into the UK economy. Digital content suppliers should retain the IP rights to the content which they produce in the same manner as TV producers.

- The BBC could play an important role as a catalyst for growth in the digital economy by opening out more opportunities to the digital sector. This should include flexibility in IP rights ownership to enable different business models to develop. This is more important than ever given that the government's policy to open up competition for BBC digital content.

IP protection

- Pact supports the recent commitments made on IP in Industrial Strategy Creative Sector Deal.

- In this agreement document (published in March this year) the government has committed to further safeguard copyright content by convening online intermediaries and rights holders to consider the need for and agree new Codes of Practice on social media and user upload platforms, digital advertising and online market places (considering legislative backstops if sufficient voluntary progress is not made by the end of 2018).

- The government has also committed to continue to address the transfer of value from the creative industries and progress work on closing the value gap at European and domestic levels which Pact also supports.

- At the EU level, government is participating fully in the DSM copyright negotiations and championing targeted measures that address fairness in the online value chain, seeking to increase revenue flows to creators. They are also seeking clarity when online service providers might be liable for content uploaded by their users without the permission of rights holders and ensuring that proposals support creators without creating unnecessary burdens for businesses. And as the UK leaves the EU the government will seek to ensure stability and certainty in the UK IP framework.

- Domestically Pact also supports the government's work on the Digital Charter which will consider legal liability that online platforms have for the content shared on their sites, including how to get more effective action through better use of the existing legal frameworks and definitions.

- Pact consider this to be the right way to tackle issues concerning rights holders with regards IP infringement. This will guarantee the platforms to the table to discuss ways to improve the processes already in place rather than implement legislation straight away.

- It is in Platforms interests to build trust in this area especially given the recent revelations on both YouTube and Facebook where by data is being misused or questionable content is being shown next to brand advertising. As a result brands are starting to become more aware of the need to manage public perception. More and more liability for user content is being examined and platforms will want to go down the route of mediation before turning to legislation

April 2018

William Perrin and Professor of Internet Law Lorna Woods, University of Essex – written evidence (IRN0047)

Written evidence to be found under Professor Lorna Woods

Policy Exchange – written evidence (IRN0072)

1. Policy Exchange is an independent, non-partisan educational charity seeking free market and localist solutions to public policy questions. Charity Registration Number 1096300. This submission has been prepared by the Security and Extremism Unit, led by Dr Martyn Frampton and Hannah Stuart. It focuses on the first question posed by the inquiry and draws primarily on our 2017 report, *The New Netwar: Countering Extremism Online*.[1038]

Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

2. Internet regulation is one of several policy options put forward by Policy Exchange to bring about a reduction in the availability of extremist material online. This issue is vital to UK national security: the terrorist attacks in the UK in 2017 underline the seriousness of the threat from online extremism, with online radicalisation playing a role in each case.

3. There is a serious concern that we are losing the battle against internet-based extremism. To date, there has not been a single direct referral to British police by any social media company about potential terrorist content.[1039] Over two-thirds of individuals involved in Islamist terrorism offences in the UK consumed extremist or instructional material almost exclusively online, and the internet is increasingly cited as a major site for radicalisation in offenders' backgrounds.[1040]

4. Counter-terrorism officials believe that the increased prevalence of extremist material online has created a permissive climate for terrorism and increased the reach of dedicated radicalisers. Speaking at Policy Exchange, former Metropolitan Police Assistant Commissioner and Head of National Counter Terrorism Policing Mark Rowley warned of the "chronic threat" of extremism, which reaches "into our communities through sophisticated propaganda and subversive strategies creating and exploiting vulnerabilities that can ultimately lead to acts of violence and terrorism".[1041]

5. Much of this propagandising takes place online. Policy Exchange's *The New Netwar* analysed Islamic State's online strategy and found that the group maintained a consistent virtual output between 2014 and 2017 despite the loss of territory and on-going fighting. We found jihadist content commonly being disseminated in two stages: core content is first transmitted to the vanguard

[1038] Dr Martyn Frampton, The New Netwar: Countering Extremism Online, Policy Exchange, September 2017.

[1039] 'Social media giants have made no counter-terrorist referrals to police, top officer reveals', The Institution of Engineering and Technology, 6 March 2018.

[1040] Hannah Stuart, 'Islamist Terrorism: Key Findings and Analysis', Henry Jackson Society, March 2017.

[1041] 'Extremism and Terrorism: The need for a whole society response', The Colin Cramphorn Memorial Lecture by Mark Rowley, Policy Exchange, 26 February 2018.

using Telegram, before being circulated to a wider audience by means of mainstream social media platforms such as Twitter, Facebook and YouTube. For the content analysed in our study, the UK is the fifth most frequent location from which the content was accessed (after Turkey, the US, Saudi Arabia and Iraq) – and the most frequent location in Europe.

6. *The New Netwar* suggested how the Government might pursue an approach based on 'responsive regulation' to encourage the social media service providers to live up to their responsibilities in this area. As a start-point, we argue that they should be treated as *de facto* publishers and distributors of online content – a position endorsed by the review into intimidation in public life by the Committee for Standards in Public Life.[1042] We also suggest that the Government should establish a new independent regulator of social media content – within the purview of Ofcom – as part of a graduated plan of measures that push the tech companies to take decisive action.

7. As part of the work, Policy Exchange commissioned an ICM poll on public attitudes towards issues related to extremist online content, radicalisation and possible interventions.[1043] We aimed to understand: a) the extent to which the public is worried about extremist content online; b) the degree to which there is an appetite for new approaches to this problem; and c) the way in which public views about online extremism correspond to underlying attitudes about the internet, and questions about the need for security and liberty. Overall, our polling showed that the public is convinced of the need for tougher action against online extremism – there are clear majorities for action of one kind or another, including independent internet regulation in the Ofcom model.

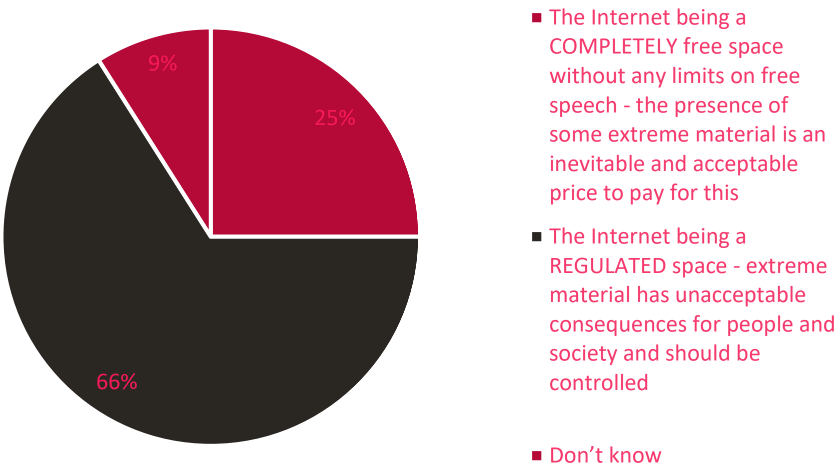
Relevant key findings include:

8. **Two-thirds public support for regulation to control extremist material online** – 66% of people believe that the internet should be a regulated space in which extremist material is controlled; only 25% feel that it should be "completely free" without any limits on free speech.

Which would you prefer?

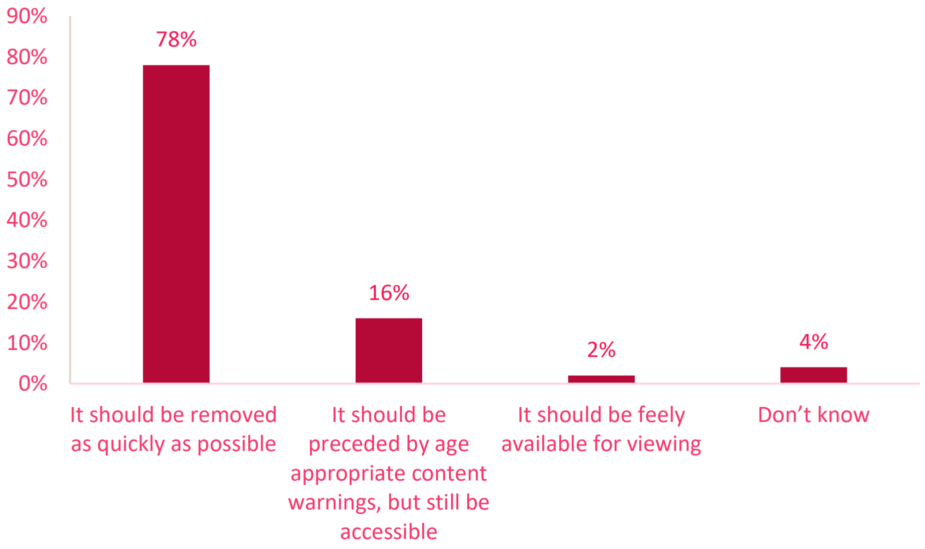
[1042] *Intimidation in Public Life: A Review by the Committee on Standards in Public Life*, Cm 9543, December 2017.

[1043] ICM interviewed a sample of 2,001 GB adults aged 18+ online, between 14th-18th July 2017. To ensure a representative sample, at the analysis stage data has been weighted to the profile of all GB adults aged 18+. A sample size of 2,001 produces data accurate to plus or minus (+/-) 2 percentage points at the 95 per cent confidence level. Survey conducted in accordance with ISO 20252 and ISO 27001, the international standards for market research and information security management. Summary available at: https://policyexchange.org.uk/wp-content/uploads/2017/09/Online-Extremism-Assessing-Public-Attitudes-Topline-Questionnaire.pdf



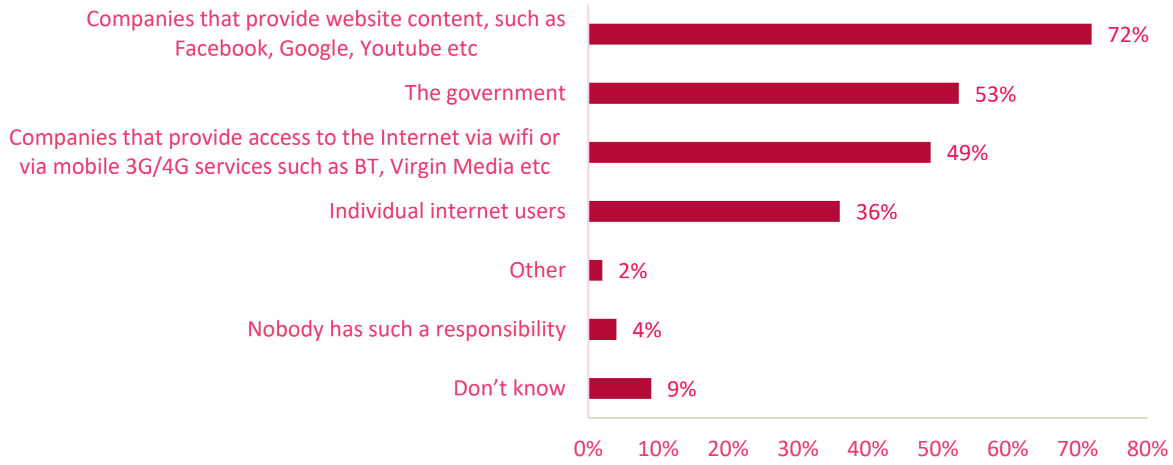
9. **Strong support for greater intervention against extremist material online** – When asked specifically how extremist material should be dealt with, an overwhelming majority favoured its removal 'as quickly as possible' (78%) from the internet. At the other end of the spectrum, just 2% of respondents felt that extremist content should be 'freely available' for viewing.

What do you think is the best way in which extremist material should be handled on the internet?



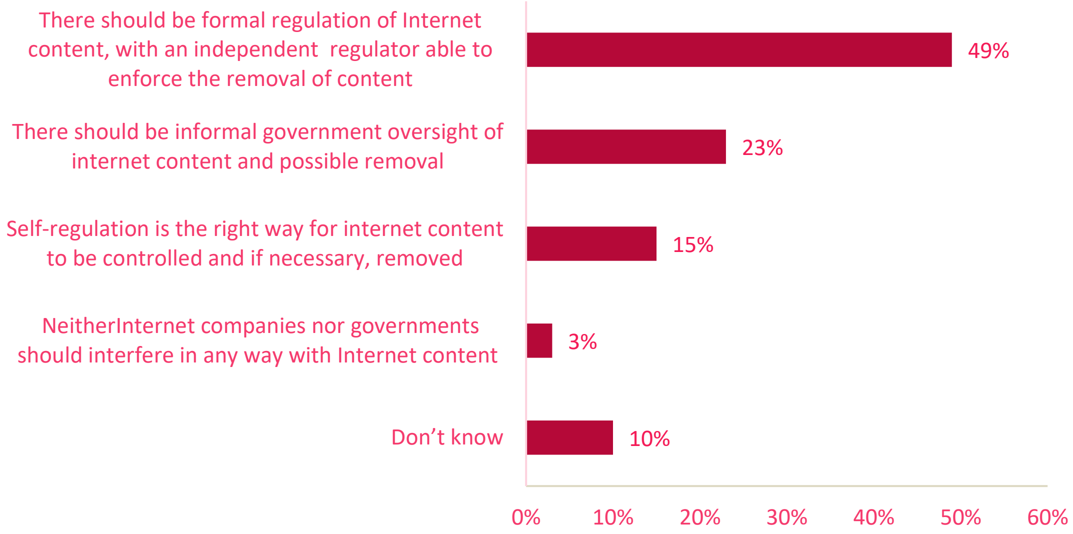
10. **Responsibility for responding to extremist content online** – When asked who was responsible for controlling, or removing, extremist content, by far the most popular answer (72%) was 'the companies that provide website content, such as Facebook, Google etc'. Respondents could give more than one answer and other popular options were: 'the government' (53%); 'the companies that provide access to the internet (49%); and 'individual internet users' (36%).

Who, if anyone, do you think has responsibility for controlling – or removing – extremist content that can be accessed online?



11. **Preference for independent regulation over self-regulation by internet companies** – When asked for their views on different ways in which the internet might be regulated only 15% of respondents expressed support for self-regulation of the kind that currently exists. Twenty-three per cent said that there should be informal government oversight of internet content, with the provision for content removal – while 49% favoured formal regulation of internet content, via the creation of an independent regulatory body, which would have the power to enforce content removal.

On the subject of internet regulation, what do you think are the best options?



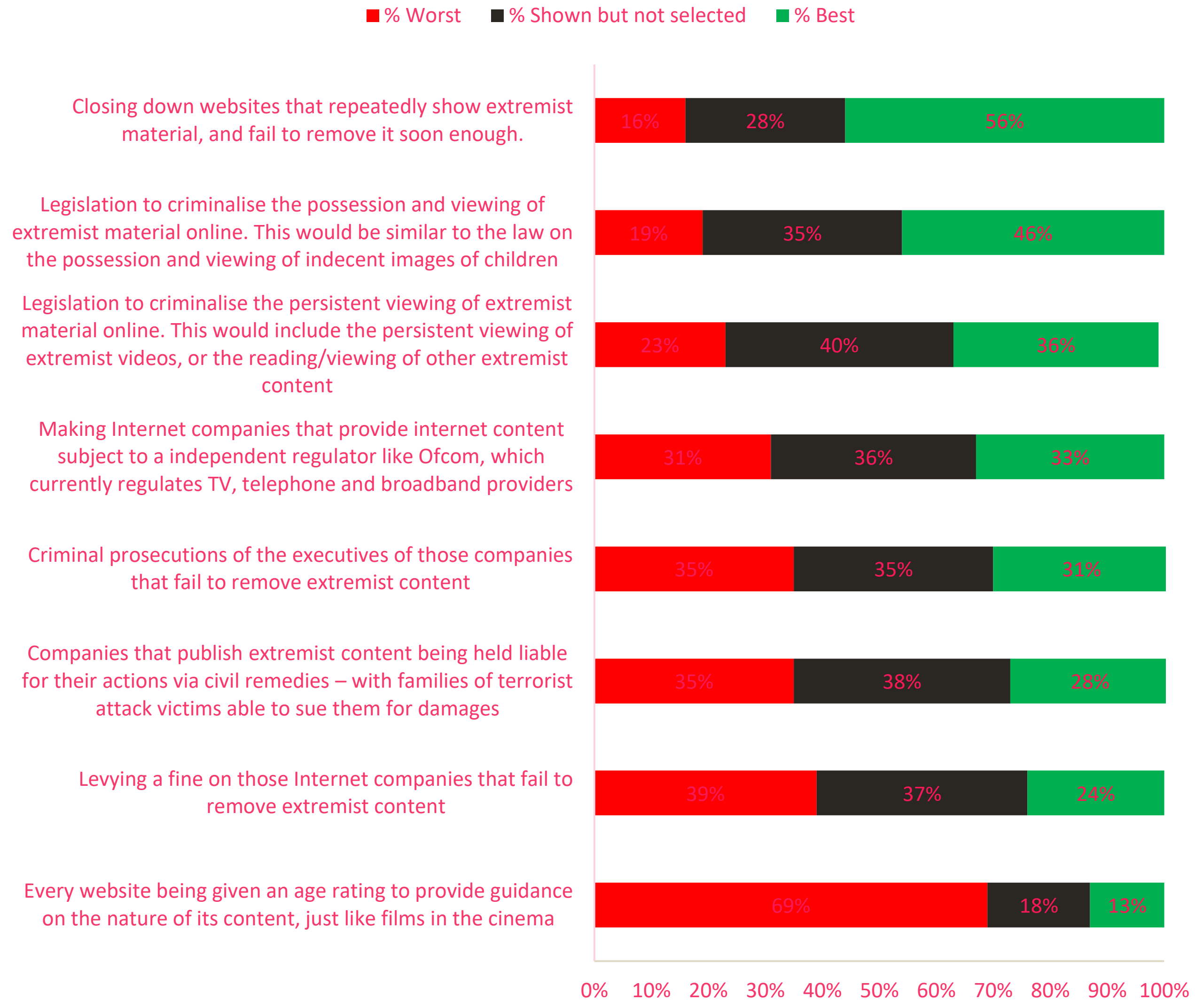
12. **Strong public support for possible interventions** – There is majority public support for a range of potential measures for tackling online extremism. 75% of respondents said they supported an independent regulator in the Ofcom mode; just 6% of people opposed this idea.

Proposal	Strongly support	Tend to support	Neither	Tend to oppose	Strongly oppose	Don't know
Closing down websites that repeatedly show extremist material and fail to remove it soon enough.	60%	21%	10%	3%	1%	5%
	NET: 80%			NET: 5%		
Levying a fine on those Internet companies that fail to remove extremist content	52%	26%	11%	4%	2%	5%
	NET: 77%			NET: 6%		
Legislation to criminalise the persistent viewing of extremist material online. This would include the persistent viewing of extremist videos, or the reading/viewing of other extremist content	46%	28%	13%	4%	3%	7%
	NET: 74%			NET: 6%		
Legislation to criminalise the possession and viewing of extremist material online. This would be similar to the law on the possession and viewing of indecent images of children	46%	27%	14%	4%	3%	7%
	NET: 73%			NET: 7%		
Making Internet companies that provide internet content subject to a independent regulator like Ofcom, which currently regulates TV, telephone and broadband providers	41%	34%	13%	3%	2%	7%
	NET: 75%			NET: 6%		
Companies that publish extremist content being held liable for their actions via civil remedies – with families of terrorist attack victims able to sue them for damages	37%	26%	17%	8%	3%	8%
	NET: 64%			NET: 11%		
Criminal prosecutions of the executives of those	36%	29%	18%	8%	3%	6%

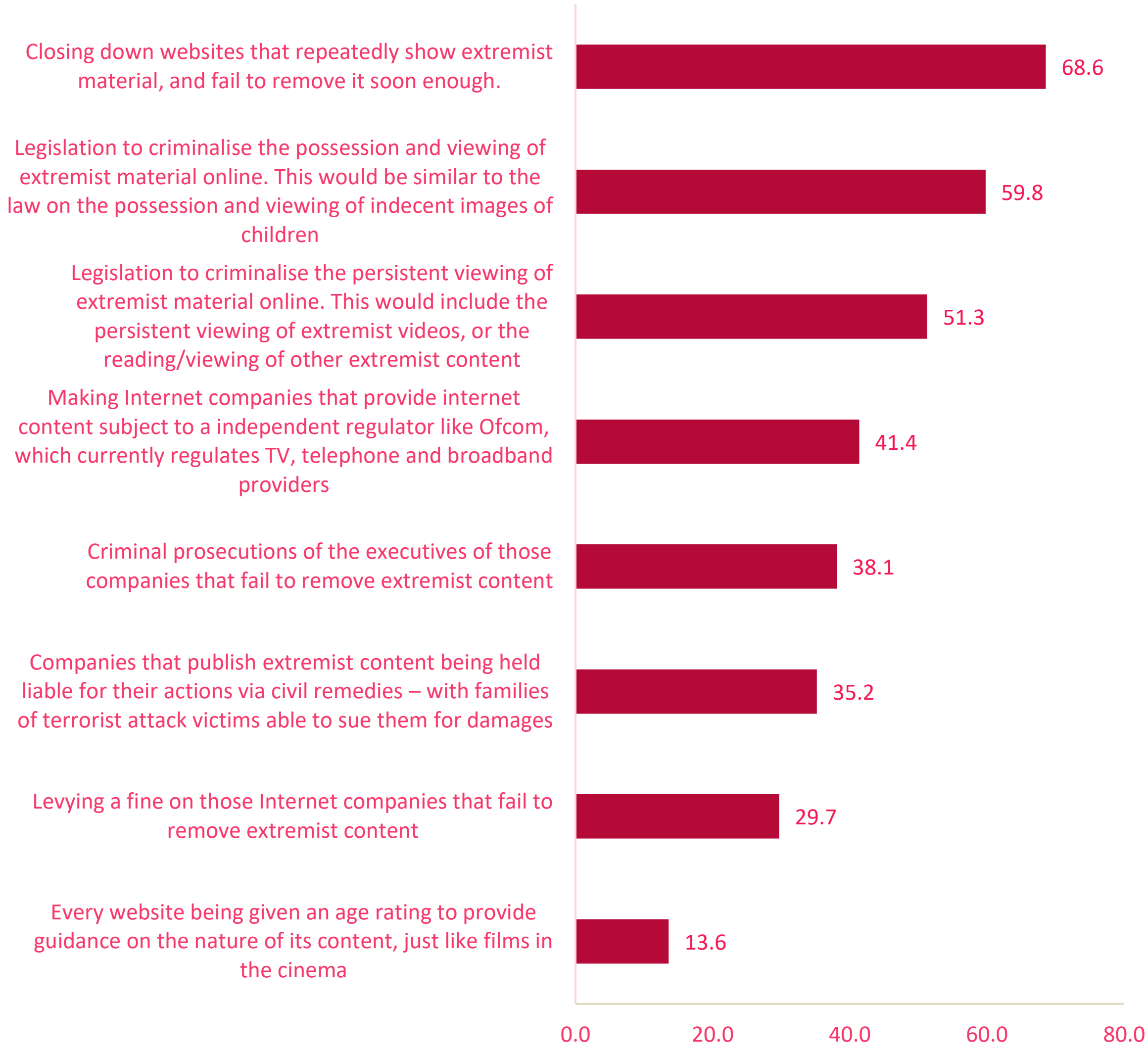
companies that fail to remove extremist content						
	NET: 65%			NET: 11%		
Every website being given an age rating to provide guidance on the nature of its content, just like films in the cinema	32%	30%	22%	6%	3%	7%
	NET: 62%			NET: 9%		

13. Since all the proposals listed garnered majority support we sought to establish preferential views of the proposals, with each ranked in relation to the others. To this end, we offered participants three options in a succession of questions, and they were asked to pick the best, the worst (and leave one). We applied a MaxDiff statistical process to the results, which established a hierarchy of preferences. Independent regulation (in the Ofcom mode) was the fourth most popular of eight options. The full hierarchy is as follows:

Number of wins



Importance scores



May 2018

Procter & Gamble – written evidence (IRN0104)

About Procter & Gamble (P&G):

1. P&G is one of the world's largest consumer goods companies and the Company behind favourite household brands such as Gillette, Ariel, Pampers, Olay, Fairy and Oral-B. Originally founded by an Englishman and an Irishman, we're proud of our local heritage.

2. Globally, P&G has around 95,000 employees with operations in around 70 countries. Our brands are sold in 180+ countries in the world. P&G entered the UK market with an acquisition of Thomas Hedley & Co in the 1930s – P&G's first international acquisition outside of North America.

3. P&G employs around 4,000 people in the UK & Ireland and has 12 sites, including Business sites, R&D Innovation Centres and Manufacturing Plants/Distribution Centres.

4. At P&G the consumer is boss. Everything we do starts and finishes with them. Our business model is simple:

    1. We identify insights from talking with the consumer on what their needs are;

    2. We use this consumer knowledge to innovate and produce quality products;

    3. We create advertising to let consumers know about these products and their benefits; and

    4. Consumers buy our products, use them and provided they deliver on their promises – as communicated in advertising – consumers re-buy, rewarding us with their loyalty.

5. P&G generally appears in the top 10 advertisers, by spend, when considering advertising across all mediums, in any given quarter. Our annual UK advertising spend is over £200 million and digital is in our top four investment choices alongside other mediums such as TV, radio, print, cinema and outdoor.

6. As a member of ISBA we are in support of the recommendations shared in their submission to the Committee. In addition to this, we have some additional observations which this submission focuses on that are specific to the areas of interest most pertinent to our consumers, and with the lens of the role of any internet regulation on digital advertising.

Regulatory Overview:

7. Whilst internet activity, in all its variance, is already covered by a broad set of legislation at both a domestic and international level, we at P&G believe the current *status quo* is not acceptable and needs attention. Consumers also perceive it to be less well-regulated than other channels.

8. P&G firmly supports the right of consumers to have their data properly safeguarded and privacy respected: a position we have held for a long time. As a responsible advertiser, we welcome the recently introduced EU General Data Protection Regulation (GDPR), which strengthens the law on data protection and privacy for all consumers within the European Union.

Post Brexit:

9. We, like ISBA, recognise and welcome the UK Government's intent to align data legislation with the provisions of GDPR through the Data Protection Bill 2017.

10. We refer the Committee to our comments and concerns previously raised under its inquiry into UK advertising in a digital age.

11. At P&G everything we do starts and ends with the consumer. It is important that we are able to develop products, brands and advertising that are locally relevant to a UK consumer. As a multinational company, maintaining alignment post Brexit in key directives across data protection and e-Privacy, is therefore critical. The UK's continuing leadership position in, and reliance on, digital advertising will be dependent on the continuing free movement of data between the UK and the EU.

Independent Self-Regulation of Digital Platforms:

12. We very much echo ISBA's concerns with the digital advertising supply chain in its current format, and have vocally and proactively supported the drive for improvements to be made across all parts of the chain, led by our Chief Brand Officer, Marc Pritchard, with his first industry disrupting speech on this topic in January 2017. We want advertising to be a force for good for society and a force for growth.

13. At P&G we firmly believe that across any medium, the advertising content consumers see must be **legal**, **honest**, and **truthful** as advocated by the regulator ASA. Alongside this, it needs to be served to them in mediums that can be trusted. We believe that, as with all advertising, the content of the advertising and the advertising platforms – which includes traditional channels, publishers and social networks – need to hold themselves accountable. Otherwise, consumers will lose trust in the brands, in the advertising and in the platforms.

14. Whilst the ASA have made great progress regulating digital advertising we still consider there is an erosion of trust in digital advertising amongst consumers due to several factors. We do not believe that digital advertising has strong enough boundaries in terms of the volume of advertising served to consumers, placement of that advertising, or its format, in the same way that TV, radio, print and outdoor do. Digital advertising can therefore be obtrusive and interrupts consumers in unwanted ways.

15. At P&G we have always held ourselves accountable to ensure our advertising reaches the same high standards irrespective of the medium it is placed in. We hold all our advertising, whether it is native or influencer, to the same high standard of broadcast advertising and ensure that it is clear to the consumer and in compliance with the regulators.

16. When it came to the eroding trust in digital advertising, P&G saw it was time to take action. The steps we are taking are five-fold:

    1. We said that the industry should move to one viewability standard so we know whether an advert has the chance to be seen.

    2. Demanding independent third party accredited verification on all our digital advertising so we know that we are achieving the media reach and frequency that we have paid for.

    3. Reinventing agency partnerships and ensuring we have transparent agency contracts so we know how our agency partners are spending our money.

    4. Ensuring brand safety so that we know our adverts show up in the right environment, not alongside content that is alarmist, controversial, or inappropriate.

    5. Insisting on eliminating advertising fraud so we know that humans, not robots, are seeing our adverts. At P&G we have decided that this is an area for outside experts who have a much higher probability of staying ahead of the criminals than we as a business ever will. We would direct the Committee to ISBA who can provide further perspective on what is happening in this area.

17. P&G is not alone in this journey, and efforts to transform the industry will require partnership and collaboration across the industry (i.e. all brands and businesses that advertise or provide a context in which to do so). We are therefore supportive of ISBA's call on the digital platforms to consider the establishment of an independent body to provide oversight of content policies and their implementation on their platforms if it is funded well, and appropriately staffed. This should be complimentary to the existing work the ASA is undertaking to support regulation of this space.

18. We refer the Committee to page 4 of ISBA's submission for further detail on the parameters for this.

Brand Safety:

19. At P&G we have zero tolerance for our adverts being associated with violence, bigotry or hatred. Brands are judged by the company they keep, which is why we have insisted on brand safety so we know our adverts show up in the right place, and not in or next to objectionable content. When platforms cannot deliver this, we remove or suspend placement of our advertising until it has been resolved. There is still work to do across the industry, but we are encouraged by the progress made over the past year to clean up the digital media supply chain - driven by the entire industry stepping up to take action.

20. We are supportive of ISBA in their ongoing commitments on behalf of the industry to maintain a proactive and robust dialogue with the digital industry to take appropriate action. We would direct the Committee to page 5 of ISBA's submission for further detail on the important work they are also undertaking here.

June 2018

Professor of eGovernance Lilian Edwards[1044] – written evidence (IRN0069)

Summary

What should the legal liability of online platforms be for the content that they host?

- Legal regimes to set a balance between the liability and exposure to risk of platforms and the interests of users, rightsholders and society, already exist, in Europe, in the form of the Electronic Commerce Directive (ECD) arts 12-15. These deceptively simple rules were actually the result of hard-fought compromise to reach a global consensus on a regime which would simultaneously promote Internet innovation and social benefit, while not disregarding the needs of users and rights like freedom of speech. We should be slow to throw this consensus away in the rush to put liability on platforms to deal with admittedly pressing new threats like hate speech and fake news online.

Online content moderation issues

- Targets for removal of content within 24 hours, or 2 hours, or less, however vital they seem to social protection, will have perverse consequences in making unfettered automated moderation, filtering and blocking the norm, done cheaply and without safeguards.

- Removing limited liability as above in the belief platforms now have access to perfect magic "AI" tools which can accurately, speedily and cost free remove all offending content would also be misguided.

- Algorithmic moderation has very many problems around bias, error, history of training data, cultural differences, semantic vagueness, et al
- Transparency in moderation rules (including "rights to an explanation") is not enough to preserve equity, due process and free speech online. We need better ADR and challenge solutions for users; standards for content moderation; state oversight, perhaps including an Ombudsman; international harmony in guidelines/new laws.

Dealing with platform dominance and lack of competition

[1044] Professor of E-Governance, University of Strathclyde, Glasgow.

- Legal solutions such as competition law actions are on historical evidence, likely to be long drawn out and less successful than technical solutions, which should at least be promoted alongside.

- Data portability under GDPR is helpful to break platform power and protect user privacy but what is really needed is regulation for *inter*operability. Research on edge computing needs integrated into mainstream debate on platforms and privacy regulation.

- Tools to come in the E-Privacy regulation, if the UK chooses to accept it post Brexit, may help to move platforms towards subscription business models, and away from the data-driven business models which have created the current profiling and privacy "surveillance capitalism" problems. Evidence from music streaming is that this is not unthinkable.

2. What should the legal liability of online platforms be for the content that they host?

1. The main legal tool to date with which platforms and intermediaries have been regulated has been the threat of liability for the content they host. Content often carries with it legal liability, which may be civil or criminal. The lack of harmonisation on this across countries and content sectors in the late 90s and dot-com boom period lead to calls from industry for some form of rescuing certainty in the form of special statutory regimes. The E-Commerce Directive (ECD) 2000 alongside the Digital Millennium Copyright Act (DMCA) in the USA effectively established the ideas of limited liability and "notice and take down" (NTD) as the template for intermediary responsibility, an idea which had remarkable reach for over a decade and remains the pattern of many OECD laws[1045].

2. This paradigm rested mainly on three justifications put forward by the emergent Internet service provider industry:

    a. lack of *effective legal or actual control*
    b. the *inequity* of imposing liability upon a mere intermediary ("shooting the messenger"),
    c. and in Europe especially, *consequences* for the public interest if unlimited liability was, nonetheless, imposed.

3. In the US, a combination of historical accident, combined with the desire to preserve free speech online, ramming headlong into domestic pressure to crack down on Internet piracy in music and films as well as child access to online porn, lead to the creation of two quite separate regimes of

[1045] See *THE ROLE OF INTERNET INTERMEDIARIES IN ADVANCING PUBLIC POLICY OBJECTIVES*, OECD, 2011 at https://www.oecd.org/internet/ieconomy/48685066.pdf.

immunities for intermediary liability, one the DMCA a limited liability/ NTD paradigm akin to the ECD, but the other, the Communications Decency Act s 230 © provided total immunity to service providers (SPs) in respect of content provided by persons other than the SP. This applied re all content other than intellectual property (IP) and federal crimes (eg possession of child pornography).

4. While all of these have been reviewed in recent times with a sceptical eye (and s 230 (c) especially is regarded as leaning too far towards protection of intermediaries) , there is some global academic and industry consensus that all three of these statutes created a global climate in the last 20 years or so in which (a) an innovative internet industry was allowed to thrive without constant fear of overwhelming risk (b) free speech online was to some extent preserved (c) interests of "victims" such as rightsholders were reasonably balanced against the immunity to risk of the SPs and (d) social benefit in innovation and access to free speech online was this also promoted. In short the ECD and DMCA especially offered good solutions to a very conflicted balance between the power of platforms and the public interest.

5. This hard-won and working consensus is now too easily being forgotten as the system comes under enormous pressure from roughly three directions. The first of these for a long time has been the P2P "piracy" wars where IP rights holders have sought to make platforms responsible for policing copyright infringements. More recently however the two key pressures have been: the rise in "hate speech" and racial and religious tension in the wake of recent Islamist fervor, post-recession immigration crises, the rise of extremist political parties throughout Europe etc. The second is the rise of "fake news" and the claims especially that it has destabilised democratic elections.

6. It is easy and tempting to ask platforms to clean up messes which they have to some extent created, to some extent arguably profit from and which they seem to have the best ability to fix. But these solutions often involve inadvertent consequences. An increasing trend is towards imposition of hard time limits to meet social goals, notably in the area of hate speech, including racist and anti-semitic speech. Notoriously, in 2017, the German Netzwerkdurchsetzungsgesetz (NetzDG) law demanded that platforms with more than 2 million users (aimed, obviously, at Facebook, Instagram et al) removed "obviously illegal" hate speech posts within 24 hours or be fined up to 50 million Euros[1046].In March 2018 the Commission issued a series of "operational procedures"[1047]. These included, radically, the demand that all companies should remove "terrorist" content within one hour from its

[1046] See "Verboten: Germany's risky law for stopping hate speech on Facebook and Twitter", *New Republic*, 3 April 2018 at https://newrepublic.com/article/147364/verboten-germany-law-stopping-hate-speech-facebook-twitter.

[1047] See http://europa.eu/rapid/press-release_IP-18-1169_en.htm.

referral as a general rule. These kinds of demands have been echoed by UK ministers recently. Furthermore Matt Hancock has referred several times to the fact that the protections of the ECD might be weakened or removed after Brexit. In my opinion this should be thought about very carefully.

3-7 Online content moderation by platforms issues

7. The paradigm I mention in 2 above has recently been repelled mainly by the belief that "AI" or automated algorithmic moderation can be a silver bullet, quick, cheap and capable of removing harmful content before it can pollute society, radicalise, upset children etc. Platforms could handle volumes of take down requests and move to pre-emptive filtering without overwhelming costs and risk. However AI (actually machine learning based on historic data) is not such a silver bullet.

8. The emphasis on speed mentioned in 6 above especially has lead to an inevitable promotion of algorithmic filtering systems. But these show worrying tendencies. First it is known that high rates of error, discrimination and bias are found in these systems and that they are typically opaque, do not generate explanations of decisions and are difficult to audit or challenge[1048]. Daphne Keller (previously head of intermediary liability at Google, now Stanford) recently said on Twitter: "The thousands of moderators who judge our social media posts are making those snap judgments at a rate of once every ten seconds. It's like the biggest implicit bias experiment ever – one that includes our every online utterance."

9. Machine learning (ML) specialists anecdotally reckon that an automated system will probably have around a 90% success rate, depending on the training set and the case being classified. Both false negatives and false positives are inevitable. Classification of semantically or contextually ambiguous material such as breastfeeding pictures or "satirical" racist jokes is extremely difficult. We also do not generally know behind the veil of corporate secrecy how (or where) the system was initially "trained" and whether the human raters who provided data were standardised, biased or appropriate[1049].

10. Secondly, enforcement is being pushed on to the private sector, in the form of the traditional scapegoats, the large US social media platforms, and away from local governance and community enforcement where local cultural concerns might be better implemented. Thirdly, the combination of private platform governance and automated management of take downs leads inevitably (as will be shown in the case of copyright takedowns below) to a failure to consider defences or mitigations in respect of the content – most

[1048] See generally Edwartds L and Veale M "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For" (2017) 16 Duke Law & Technology Review 18.

[1049] See discussion in R Binns et al "Like trainer, like bot? Inheritance of bias in algorithmic content moderation", 5 July 2017 at doi: 10.1007/978-3-319-67256-4_32.

notably, whether freedom of speech, or religion and perhaps of political discussion and assembly are being bulldozed under in the rush to meet removal targets and avoid regulation or fines.

11. There are partial solutions here which should be encouraged. More transparency, as recently seen in the form of the publication of FBs content moderation rules and YouTube's take down "flags" is helpful and emerging driven by recent PR scandals eg Cambridge Analytica. But it is still unclear what action could be taken if the processes revealed seemed socially unacceptable either by governments or users, bar long and precarious challenges on human rights grounds.

12. If we are to move to an information society of automated privatised content censorship, and furthermore incentivise it with extremely fast take down targets, and heavy penalties for unmet targets, there must, urgently, be safeguards put in place. One way forward might be to regulate Facebook as a kind of public forum or utility, with minimum transparency, due process and oversight rules; but a new paradigm needs constructed here, not simply borrowing from the status of a commercial or PSB broadcaster. Another might be to require a low cost or free ADR system for users, of the sort companies like eBay have provided in the past, but with public oversight or audit (an Ombudsman for Facebook?). Attention should be paid to the recent Santa Clara Principles on Transparency and Accountability of Content Moderation[1050]. But it may also be necessary to declare that a certain percent of moderation must involve human checks, even if it costs, and/or that certain types of training or certification are required. Transparency alone, and leaving matters to unaided user action, are not enough.

13. On the other hand simply dumping full liability onto platforms, for the reasons discussed in paras 2-4 is also not sensible. We need to construct a new consensual compromise, ideally globally, not rush into a series of national or regional panic and partial measures, which may reduce innovation, alienate socially useful services (think of the retreat of Google News from Spain), or, most likely generate illusory but box-ticking solutions, such as more transparency or better privacy policies that no one reads. Around 2010 there was considerable global activity between the European Commission, OECD, WIPO, US state depts etc to try to re-establish a global compromise. This time round however the domains have become fragmented and heavily politicised and there is a worrying lack of cross-national discussion. This should be promoted, at industry, academic and policy levels.

8. What is the impact of the dominance of a small number of online platforms in certain online markets?

[1050] https://newamericadotorg.s3.amazonaws.com/documents/Santa_Clara_Principles.pdf.

14. I do not intent to quantify this impact – others will do that better - but to suggest some solutions to what are clearly (IMHO) bad effects on free speech, privacy, democracy and online safety caused by the current platform economy and in particular, the "free to users, but revenue from targeted ads" business model. It is well known that network effects tend to drive towards a monopolistic effect in sectors like social media and search which ordinary competition struggles to break. Incumbent platforms also benefit from the proprietary data siloes they build up as a result of their control over the market. Hence more privacy protective rivals to FB, Google etc continually fail to thrive. How do we deal with this?

15. Competition law is one obvious way forward and various writers are promoting solutions involving eg breaking up Facebook or Google, by region, activity or otherwise. The problem with these is that competition law at this scale is a very slow and blunt instrument which has historically failed to really solve information monopoly problems.

16. A partially technical solution with great promise is the promotion of personal data containers (PDCs) or "edge computing". The idea here is that instead of users contributing their data to platforms, who then provide services like search or social networking, the user keeps their own data and applies processes to it (perhaps from a special "app store"). This enables them to get the social benefits of current platform services without (a) contributing to the power of these platforms and especially (b) without compromising their privacy and enabling the kind of profiling and tracking which is now universal. These ideas currently only really exist at research level but I draw the Committees attention towards one excellent attempt in this area known as Databox[1051]. Such solutions are also helped serendipitously by the recent arrival of the right to data portability in art 20 of the GDPR. This right should be promoted and research in this area supported.

17. Data portability is not however enough to limit platform power and control over user data in contexts like social networking. Users will not leave platforms where all their friends are unless they think they can continue to interact with them. What they need is data *interoperability* for this. Colleagues at CREATe and Horizon Digital Economy Hub tried to create tools to "interoperate" with FB during the CREATe project but found it impossible because FB constantly changes its APIs to repel boarders. Regulation to promote true interoperability is vital as the market alone will always reject it as a threat to proprietary advantage. Again a debate is needed on how best to incentify interoperability; law, technical standards, competition remedies, tax breaks, what? One possible future could involve using portability and interoperability to wean users from platforms like FB to independent not for profit platforms (or to allow them to co-exist across

[1051] See https://www.databoxproject.uk/ for details.

both).

18. A final brute force way to rectify the power of platforms in terms of their collection of personal data and profiling, is to incentify a move towards subscription fees rather than advertising revenue. Regulation to push this may be arriving in the form of the new ePrivacy Regulation (likely to arrive after Brexit?) which may yet ban the likes of FB from requiring consent to tracking as the price of entry. Even if the EPR does not in the end go this far it is something which we should start to think about. In domains like music streaming, Spotify has shown that users can be weaned from a free ad-supported business model to a subscription model with fair success. Problems still arse from this: should privacy become a luxury good? But there are also economic reasons to worry that the entire information society cannot be supported forever on advertising revenue alone.

11 May 2018

Radiocentre – written evidence (IRN0048)

INTRODUCTION

1. Radiocentre, the industry body for commercial radio, welcomes this House of Lords Communications Committee inquiry on the question of internet regulation. The growth and development of the internet in recent years has undoubtedly enriched people's lives by providing access to limitless information, open communication and entertainment, but the extent and speed of this transformation has made it difficult to fully appreciate the consequences of such a seismic change.

2. As well as providing these many individual and societal benefits the rapid expansion of the internet has also provided a platform for illegal, misleading and abusive content on an unprecedented scale. In addition it has facilitated the harvesting of personal data on a scale that was unimaginable previously, mainly for commercial and advertising purposes but also to influence actions and opinions of people in other ways.

3. Until now there appears to have been a reluctance to tackle the complexity and practical difficultly of regulating the internet in any meaningful way. To some extent this is understandable, especially at the point when internet businesses were becoming established initially. However this position is becoming increasingly untenable as the power of online platforms, such as Google and Facebook, becomes ever greater and the implications of this power and dominance become clearer, whether in terms of the personal privacy of individuals, the spread of harmful online content or their near monopoly of online advertising.

4. This short response does not attempt to address all of these issues and the full range of questions posed by the Committee in its call for evidence. Instead it provides background on commercial radio in the UK; our view on regulating media content online; and our views on regulating internet advertising.

5. In particular, we highlight some of the key challenges and implications, while proposing greater consistency in approach to the regulation of offline and online content. In the short term this implies greater effort by industry to introduce effective self-regulation, backed up by Government action and legislation if this proves necessary. As a body representing broadcasters and media companies this is our core area of interest and knowledge, rather than the broader data protection and privacy issues on which the Committee will undoubtedly receive many expert submissions.

COMMERCIAL RADIO IN THE UK

6. Commercial radio is funded entirely by advertising and operates in a highly competitive market, generating over £679m in revenues in 2017. 35 million people listen to commercial radio's mix of music, news, travel and local information every week. It also supports £683m in gross value added to the UK economy and over 12,000 jobs.

7. In common with many other business sectors and areas of public life, the growth of the internet has transformed the world in which radio and media companies operate, creating a huge range of new opportunities while presenting numerous complex challenges. In particular there has been a significant shift in advertising revenues to online platforms. In the last 20 years digital advertising has grown from around 1% to a more than 50% share of UK ad revenue. This transition of ad-spend to online is the most significant economic trend that has put pressure on revenues across all media. These changes have seen radio's share of ad revenue decline since the early 2000s.

8. In addition competition for audiences has never been more intense due to the range of entertainment options now available. Online services like Spotify and Apple Music now account for a 23% share of overall listening time according to Ofcom (higher among younger listeners). This fragmentation has had limited impact on total audience, but average time spent listening to radio has reduced from 24.4 hours per week in 2004 to 21.3 hours in 2017.

9. It is also the case that this digital disruption has provided radio and media companies with opportunities to innovate, with new revenue streams, access to data and ways of providing consumers with access to content with greater functionality. Established media platforms and brands also have the competitive advantage of being highly trusted by consumers to deliver reliable news and information, while being a safe environment for brands to advertise their products and services.

REGULATING MEDIA CONTENT ONLINE

10. The overall impact of the internet on the media landscape has been well documented (including in the House of Lords Communications Committee's own reports[1052]). The spread of high-speed internet access in homes and on mobile devices has led to an explosion of entertainment choices for consumers. The unprecedented range, choice and volume of content available has led to fragmented audiences for traditional media platforms and increased the level of competition for people's time and attention. These developments have been overwhelmingly positive for consumers, with access to this content

[1052] Lords Committee on Communications report 'UK Advertising in a Digital Age' (April 2018) generally free at the point of use (funded by digital advertising) or available at relatively low cost.

11. As well as providing these many individual and societal benefits, the rapid expansion of the internet has also provided a platform for illegal, misleading and abusive content. The work of the Lords Communications Committee and the House of Commons Committee on Digital, Culture, Media and Sport (DCMS) in highlighting these issues and calling digital platforms to account is most welcome. For example, the ongoing DCMS Committee inquiry into 'fake news' on social media and the internet has explored fundamental questions regarding the responsibility of digital service providers and aggregators for content published on their platforms.

12. The spread of this type of content is potentially a threat to democracy when used in a co-ordinated way, but it may also present an opportunity for established media platforms and brands, which have the competitive advantage of being highly trusted by consumers to deliver reliable news and information. Despite (or perhaps because of) the spread of fake news online, the public see regulated platforms like radio and TV as the most trusted sources of news and information. In November 2017 the Rt Hon Matt Hancock MP, now Secretary of State for Digital, Culture, Media & Sport, took part in a launch event for Radiocentre's latest research, *Breaking News*[1053], which explores an industry-wide perspective on listeners' views on news and trust across all media.

13. While each media has particular strengths in terms of roles and consumption, radio is considered the most trusted medium in an era of fake news and is consistently found to be the most trusted source of news and information available to audiences in the UK[1054] and Europe[1055]. In Radiocentre's survey 77% of people said they see radio as a trusted source of national news, more than any other media. Just 15% of listeners trust social media for national news.

14. Against the backdrop of the issues raised in this submission, audience levels of trust, underscoring the huge gap between traditional and online media, are not particularly surprising. Traditional media have spent decades building trust with audiences within a regulated environment (currently Ofcom for broadcast, IPSO for press) and remain the go-to sources for trusted information. Social media is an important and growing part of everyday media consumption in 2018, but these sources are largely unregulated and still have a long way to go to improve their reputation for reliability and accuracy.

15. Part of the solution to these challenges must be for online platforms to work with Governments and regulators in moderating the content they make

[1053] Radiocentre report 'Breaking News: How listeners value commercial radio news' (November 2017)
[1054] Ofcom survey 'News consumption in the UK' (June 2017)
[1055] European Commission (Eurobarometer 86, 2017)

available, using a combination of technology, editorial judgement and feedback from users. However this type of self-regulation risks falling short if it lacks meaningful accountability or oversight, with no sanctions in place for persistent or ongoing problems.

16. In terms of the regulation of entertainment content, it is becoming increasingly untenable to argue for entirely different regulatory regimes based solely on the fact that distribution methods happen to be different. The fact that audiovisual content from Netflix, Amazon or YouTube is not subject to any significant content rules, yet are available alongside output from highly regulated services from the BBC, ITV or Channel 4 is already a matter of tension and confusion for audiences. A recent Ofcom survey found 4 out of 10 people believe that Netflix and Amazon are regulated by similar rules on offensive, harmful, unfair, inaccurate or biased content, with 3 out of 10 believing that YouTube is regulated in this way[1056].

17. The convergence of broadcast, online and other content is likely to accelerate even further in the next few years, making these distinctions difficult to sustain and meaningless to consumers. For example, existing radio operators are seeking to compete for audience time with digital music providers (Spotify, Apple Music) and other aggregators (TuneIn) which have no meaningful regulatory requirements. Yet commercial radio is still required to comply with legislation on content quotas and production that were devised in the late 1980s, before the internet had even been invented.

18. Last year DCMS held a consultation on commercial radio deregulation. The Government response was published in December 2017[1057] and proposed a number of sensible changes suitable for a digital future. This included proposals to end the outdated format requirements (where Ofcom determines the music output of local radio stations and operators are required to seek permission to make changes) and a focus on valuable news output rather than how and where this is produced.

19. Such changes are relatively modest compared to the task of regulating online platforms, but they represent useful accompanying measures that will assist in supporting a more level playing field in terms of future regulation. While we would not necessarily expect to see this result in complete parity of regulation between online platforms and other media (at least not for the foreseeable future), this approach will help provide a fairer operating environment, improving competitiveness and offering greater consistency in approach.

20. The time is right for a more robust approach to regulation of online content, which transfers some of the principles of acceptable behaviour from the offline word, to the online world. Alongside this “levelling up” of internet content regulation we believe that a degree of “levelling down” in regulation for

[1056] Ofcom report ‘Adults media use and attitudes report’ (April 2018)

[1057] DCMS consultation ‘Commercial radio deregulation response’ (December 2017) existing media would be appropriate, in order to reduce the disparity and recognise the trend towards ever greater convergence.

REGULATING INTERNET ADVERTISING

21. It is clear that UK businesses have been particularly keen to take advantage of internet advertising due to the potential benefits in the terms of targeting, data and apparent cost efficiency. As a result over half of UK ad spend in 2017 was devoted to digital advertising (£11.5bn), more than any other EU country and more per capita that the USA.

22. The Committee has taken extensive evidence on these issues and considered the impact of the rapid growth of digital advertising at length in its report earlier this year[1058]. This rightly identified the fundamental changes in the way that advertising is bought and sold online, with the rise of automated processes known as programmatic advertising. This process is able to use data on audiences to match the characteristics required by advertisers in order to serve relevant ads online, which can then be measured and tracked in terms of user interaction.

23. This model is clearly attractive to advertisers and their agencies who determine the vast majority of spending in this area. However, a number significant issues have arisen as a consequence of the increasing reliance on digital platforms that are largely unregulated and exempt from external scrutiny. In particular there is a lack of transparency on where the advertisers money goes (due to the cost of ad tech intermediaries); absence of agreed effectiveness measures (including third-party audience measurement and viewability of ads); ad misplacement (that can lead to ads being placed next to illegal or harmful content[1059]); and deliberate ad fraud (where web traffic is inflated and manipulated to drive false impressions).

24. A number of these areas are already subject to industry action and efforts to introduce more effective self-regulation. For example, we note the position taken by the Incorporated Society of British Advertisers (ISBA) that content should not be made available for advertising placement unless it has been positively vetted, an approach that may at least help tackle the issue of ad misplacement that can be so damaging to brands.

25. More broadly we support the recommendations made by the Committee to enable self-regulatory bodies (such as JICWEBS) to assume greater powers to create and enforce rules establishing industry standards, especially in measuring effectiveness and third-party verification. If the industry fails to do this in a manner that is satisfactory the Government should propose legislation

[1058] Lords Committee on Communications report 'UK Advertising in a Digital Age' (April 2018)

[1059] The Times 'Big brands fund terror' (9 February 2017) to regulate digital advertising, with appropriate sanctions. This approach appears to be consistent with much of the Government's thinking in its Digital Charter, which seeks to establish rules and norms for the online world and supports the principle of what is unacceptable offline should be unacceptable online.

26. In addition we agree that the Competition and Markets Authority should conduct a market study of digital advertising to consider the dominance of Google and Facebook and whether the current market is working fairly for businesses and consumers.

ABOUT RADIOCENTRE

Radiocentre is the industry body for commercial radio. We work on behalf of over 50 stakeholders who represent 90% of commercial radio in terms of listening and revenue.

We perform three main functions on behalf of our members:

- Drive industry revenue by promoting the benefits of radio to advertisers and agencies through a combination of marketing activity (e.g. events, advertising, PR, and direct mail), research, and training

- Provide UK commercial radio with a collective voice on issues that affect the way that radio stations operate, working with government, politicians, policy makers and regulators to secure the best environment for growth and development of the medium

- Ensure advertising messages on commercial radio stations comply with the necessary content rules and standards laid out in the BCAP Code of Broadcast Advertising and the Ofcom Broadcasting Code.

11 May 2018

Jacob Rowbottom[1060] – written evidence (IRN0026)

1. In this evidence, I make the following points that are relevant to questions 1, 2, 3, 5 and 7 in the Call for Evidence:

- There are both practical reasons and reasons of principle for imposing legal responsibilities on digital intermediaries. In some cases, action taken by an intermediary may be preferable to the imposition of liability on the initial author of content. (para.s 2-7)

- Intermediary regulation can raise issues under Article 10 of the ECHR. To strike a balance in determining when responsibility for content is appropriate, a number of processes and actions expected of an intermediary can be identified. (para.s 9-17)

- Regulation could be implemented by overseeing a company's internal standards and procedures ('meta-regulation') or through the direct application of certain standards (or a combination of both). (para.s 18-19)

- While there is a tendency to consider intermediary responsibility in relation to content deemed to be harmful, there is a case for more pro-active 'public service' style obligations (with election communications being a possible starting point). (para.s 20-25)

Why target an intermediary? (questions 1 and 2)

2. There are various points in the chain of communication that can be a target for regulation or legal responsibility. First, there is the liability of the initial author or publisher of the content. Second, the intermediaries (that host content, provide access, or enable users to locate content) can be held responsible or regulated. Finally, there are some controls that target the reader or viewer, such as the possession offences relating to indecent images of children, extreme pornography and certain terrorist material. Imposing liability on the viewer or possessor of content should be reserved for the most extreme material, and will not be considered further here.

3. The general approach taken in the current law is to assign primary responsibility to the initial publisher of a statement. In defamation law, an action can be brought against a digital intermediary where it is not possible or appropriate to pursue the initial author or publisher (that is reflected in sections 5 and 10 of the Defamation Act 2013). More broadly, the E-Commerce Regulations 2002 provide for

[1060] Associate Professor, Faculty of Law, University of Oxford and University College, Oxford. The evidence provided reflects the views of the author.

a scheme of conditional defences that protect intermediaries from the liabilities that are imposed on the initial publisher. In deciding whether intermediary liability is consistent with freedom of expression, the European Court of Human Rights also considers whether it is more appropriate to pursue the initial author.[1061]

4. Despite the general preference for imposing liability on the original author or publisher, there are many reasons why the regulation of an intermediary is an attractive option for policy makers. First, there are practical reasons of efficiency. If harmful material is posted and re-posted by multiple individuals, it is easier to ask a gatekeeper to control the flow of such content than to bring a legal action against each individual publisher. Moreover, the initial publisher may not be identifiable and may be based outside the jurisdiction.

5. Aside from such practical matters, there are reasons of principle for targeting the intermediary. By providing a central part of the infrastructure for digital communications and offering services that determine the visibility of content, the intermediary can share some responsibility for any harms that arise from the use of the technology.

6. In some cases, targeting the intermediary (rather than the initial author) may be the more proportionate measure. For example, a person may make a casual or ill-judged remark in the course of a conversation on the social media, which is arguably defamatory or may fall foul of a criminal standard. Imposing legal liability for every such statement would risk inhibiting the flow of everyday conversations.[1062] There are already guards against such applications of the law, such as the serious harm requirement under s 1 of the Defamation Act 2013 and the Crown Prosecution Service guidelines for social media offences.

7. Such casual comments on the social media may still have some harmful consequences. A defamatory remark or intrusive image posted online can be widely circulated, may be ranked highly in search results and potentially follow a person for years to come. The responsibility of the intermediary may strike a balance between the free flow of conversation and any potential harm. For example, a system in which an intermediary removes content or makes it less prominent could offer a compromise by allowing a speaker to say what they want without attracting legal liability or criminal sanction, while also preventing that statement unduly damaging a person’s reputation or privacy for the indefinite future. The so-called ‘right to be forgotten’ can be seen as an experiment along these lines. While there are concerns that intermediary liability or regulation can lead to a system of private censorship, it is also important to recognise that it can offer a proportionate response to some types of problem.

[1061] See *Delfi v Estonia* (2016) 62 EHRR 6 at [147-151].

[1062] This line of argument is developed in J Rowbottom, ‘To Rant, Vent and Converse’ (2012) 71 *Cambridge Law Journal* 355.

A mixed system of controls

8. Under the current system, intermediaries are subject to a mixture of legal obligations and self-regulatory measures. Sometimes an intermediary can be a 'publisher' of third party material and thereby held legally responsible for that content. The question of whether the intermediary is a publisher has generated a complex range of decisions, in which courts make (sometimes strained) analogies with traditional publishers or distributors. However, the general position is that intermediaries are subject to a system of conditional liability.[1063] Under the E-Commerce Regulations 2002, a host is held responsible only if it had knowledge of the unlawful content and failed to remove the material. Other types of regulation move away from comparisons with traditional publishers and focus more specifically on the services of the intermediary in processing information. Along these lines, the right to be forgotten established in *Google Spain* attaches responsibilities to the activities of the search engine (and not to the original publisher). The intermediary can also be subject to self-regulation, both through external bodies (such as the Internet Watch Foundation) and through the company's own internal rules. The types of control are inter-related, and the conditional legal liability provides an incentive to devise and participate in systems of self-regulation.

Article 10: Is media freedom at stake? (question 5)

9. If intermediaries that host content are subject to liability, that can raise questions of freedom of expression and media freedom. When considering duties to monitor and take down content, the European Court of Human Rights has stated that the provision of a platform 'for third-parties to exercise their freedom of expression by posting comments is a journalistic activity of a particular nature'.[1064] The Court reasoned that imposing liability on a host is to some degree analogous to punishing a journalist for reporting on the views of others.[1065] This means that any regulations or liabilities have to be compatible with Article 10 of the ECHR. The point is also important in so far as it recognises that certain intermediaries perform a type of media function in providing access to information and facilitating expression.

10. However, the protection of the hosting activity under Article 10 is conditional on the fulfilment of certain 'duties and responsibilities'.[1066] While the European Court of Human Rights has drawn an analogy with 'journalistic activity', the duties and responsibilities cannot be the same as those expected of a traditional media company. At the heart of journalistic ethics is the responsibility to verify and check facts prior to publication. That would not generally be expected of an intermediary that hosts the content of others, which it does not endorse and may not be in a

[1063] The condition can be established either in the legal definition of a publisher or through the defences available to the intermediary.

[1064] *Magyar Tartalomszolgaltatok Egyesulete v Hungary* (2016) 42 BHRC 52.

[1065] See the principle of *Jersild v Denmark* (1995) 19 EHRR 1.

[1066] The principle is well established when looking at the Article 10 rights of media bodies, see discussion in *Stoll v Switzerland* (2008) 47 EHRR 59 at [102]-[104].

position to verify. However, it can be seen that a number of duties and responsibilities are evolving that are specific to intermediary activities. These duties and responsibilities can be promoted through regulatory measures and provide a starting point in striking a balance between freedom of expression, media freedom and other competing interests.

Intermediary responsibilities (questions 3-5)

11. There are several processes and responsibilities that may be expected of an intermediary and could be considered under a system of formal regulation.[1067] Some of the examples below are already required in the existing legal framework, while others are the subject of debate. The discussion below is not exhaustive and focuses only on processes. I do not consider what sorts of content should be regulated (whether it should be limited to extreme content and the infringement of individual rights, or whether more general standards should be applied).

12. *Notice and takedown.* An intermediary can be expected to remove and disable access to material once it has knowledge of the unlawful content. Where the intermediary does not host the content, then similar controls can be taken through filtering and blocking. This process is already well developed under the E-Commerce Regulations 2002.

13. *Monitoring*. An intermediary can sometimes be expected to take positive action to ensure that unlawful content is taken down prior to receiving a formal complaint. However, under European Union law there is a prohibition on requiring intermediaries to engage in 'general' monitoring to detect unlawful content.[1068] That prohibition ensures that the intermediaries are not subject to unduly onerous requirements (given the sheer volume of content published). However, technology may address some of those concerns (for example, making it easier to detect the posting of particular types of material or photographs) and is likely to develop in future.

14. In some circumstances, a more specific monitoring obligation can be imposed, such as a requirement to block certain identified content or websites.[1069] If such obligations are to be extended or considered in a regulatory system, then a key question is what should trigger a duty to monitor (whether the intermediary knows that unlawful content is likely to be posted in a certain area) and how onerous that duty should be? The role of monitoring obligations is something that could be revisited post-Brexit (depending on the final arrangements in relation to EU law).

15. *Transparency on the criteria for blocking or take down.* The role of the intermediary in taking down or blocking content can raise issues of private censorship (in which a private company decides what content is permissible). One minimal response to this is to demand a degree of transparency. Along these lines,

[1067] This line of argument is developed in J Rowbottom, *Media Law* (Hart, 2018), chapter 7.

[1068] Directive 2000/31/EC, Article 15.

[1069] See *Twentieth Century Fox v BT* [2011] EWHC 1981 at [162].

the company can be expected to provide the criteria explaining on what basis content will be removed and blocked. Some transparency measures may go further, either by notifying a publisher when content has been blocked or removed, or informing the potential viewer why a webpage has been blocked (for example using a splash page). The expected level of transparency will depend on the legal interest and nature of the issue. A requirement to notify a publisher will be inappropriate where it infringes a privacy right, promotes evasion of a control or undermines the prevention of crime.

16. *Contesting decisions*. An intermediary may be expected to provide a right to contest a decision made in relation to the blocking or taking down of content. A key question in relation to such a process is the extent to which a system of appeal should have some independent oversight. Under some of the existing controls, there is an asymmetry. For example, if a search engine rejects a ‘right to be forgotten’ request, the complainant can take the complaint to the Information Commissioner or to the courts. The person responsible for the de-listed content, however, does not have a corresponding right and can only make a request to the operator of the search engine to reconsider the decision. Similarly, in the conditional liability scheme under the E-Commerce Regulations 2002, a complainant may bring legal proceedings to pursue the host if there is a failure to remove the content once notice has been provided. By contrast, the original publisher of the content does not normally have a legally enforceable right to challenge the intermediary’s decision to remove or block the material. The rights of the publisher to challenge a decision (while not appropriate in every case) could be a possible issue to be addressed by a regulator.

17. *Fair terms in content selection*. In relation to some services, an intermediary cannot avoid making a selection between content. Part of its function is to prioritise information in a way that is useful to users. While the decisions are normally made by algorithm, such systems can nonetheless develop biases in the way content is prioritized. One role for a regulator might be to hear complaints about any such biases and to assess whether steps can be taken to avoid any unfair discrimination in its decisions. Alternatively, the intermediary may be expected to follow certain processes of consultation in relation to its systems, or be willing to hear challenges. More broadly, there may be a case for a positive expectation for intermediaries to prioritise certain types of content (for example, whether a news organisation fulfilling certain standards should sometimes benefit from a privileged position in the ranking of material).

Methods of regulation

18. The processes outlined above could be addressed through a combination of direct regulation and meta-regulation. Under a system of meta-regulation, the regulator could oversee the internal self-regulatory systems employed by the intermediary companies. Along these lines, the regulatory body could ensure that intermediary companies have adequate policies on transparency, notice and takedown, and an appeals process. The body could check to see that the forms for reporting unlawful content allows for the necessary information to be included, and

that the process is clear to users.[1070] The meta-regulator could also ensure that the process of appeal is sufficiently independent of the initial decision-maker. Given the scale of digital publications, a regulatory focus on a company's own internal processes is likely to be an attractive option (as opposed to the regulator handling all complaints directly).

19. Leaving such issues primarily to the industry raises the difficulty of private companies deciding what content is most likely to be seen. The intermediary may not be well placed to determine whether a defence in a defamation claim would succeed in relation to third party content, or to determine whether the public interest justifies publication. In some circumstances, there is a case for a regulatory body (or a representative content panel) to provide a forum to hear certain complaints or hear appeals on some intermediary decisions. If such a regulator were developed, it could stand as a separate sector of media regulation (alongside Ofcom for broadcasters and self-regulation for newspapers) that develops specific norms and standards that are tailored to the activities of the intermediary.

Public service obligations: elections

20. Most of the discussion of intermediary responsibility tends to focus on minimising the dissemination of content deemed to be harmful. However, there is also an argument that the intermediary can play a more pro-active role in promoting certain positive outcomes. Such an approach to regulation has traditionally been applied to the broadcast media, partly on account of its capacity to reach a large audience and thereby promote a national forum for discussing public issues. Given the widespread use of certain intermediary services, an equivalent function could potentially be performed by the leading hosts, social networks and search engines. While this could be developed for various spheres of activity, elections may provide a useful case study, given that it is a defined context and takes place for a limited period of time. Moreover, election communications have been a key area of concern in relation to the digital media. There are a number of ways an intermediary could perform a public service function in an election. Below I set out some tentative suggestions.

21. *Delivering free election communications to a mass audience*. Certain digital intermediaries could offer free political messages for political parties and candidates (a digital equivalent to the system of election broadcasts). Under such a scheme, a video hosting site could require users to watch a short message before viewing the selected content. A search engine could provide links to the leading parties or candidates in response to certain queries during an election campaign (with results provided under a heading that clearly separates the 'public service results' from the ordinary search results).

[1070] **The adequacy of such forms has been criticised in the course of litigation, see *JR20 v Facebook Ireland Limited* [2017] NICA 48 at [41].**

22. The aim of such a scheme would not simply be to provide cheap advertising, but to offer something distinct from targeted paid political advertising. A party making use of the scheme could be required to offer the same message or advert across the whole country and thereby ensure that the national audience sees the same message. The scheme would also aim to ensure that voters receive communications from a range of parties. The question of allocating such free time could be decided by the regulator and the participating intermediaries (an equivalent to the Broadcasters Liaison Group). While the prospect of extending PEBs to the digital media is unlikely to generate much excitement, it is important to remember that the system on the broadcast media has been a key element in reducing the costs of an election.

23. *Transparency of election communications*. The intermediary could be required to publish information on the amount that it has been paid to carry political advertising and by whom. The intermediary may also require paid political advertisements to include a link to further information about the person responsible for the message.

24. A further way to improve transparency may be to provide a publicly accessible repository of political advertisements that the intermediary has been paid to carry (or at least of those where the level of advertising exceeds a certain threshold). Such a system could combat the concerns about micro-targeting, so that voters and monitors are able to check what the party and campaigners are saying to other demographic groups. This may not cover every type of election communication, but could enable some scrutiny of the messages.

25. *Equal opportunities and fair terms*. An intermediary offering an advertising service could be required to provide for equal opportunities in the terms and conditions for paid political advertising by parties and candidates.

11 May 2018

Royal Academy of Engineering – written evidence (IRN0078)

Summary

1. When considering internet regulation, a central question is how to maintain values such as openness, accessibility and universality – and correspondingly, the essential attributes of the internet - while minimising the harm that misuse of the internet has the potential to inflict.

2. A key challenge for implementing regulation or other types of measure is that the internet itself is evolving: both the underlying technologies and the ways in which they are put to use. The internet of the future will increasingly be powered by data and algorithms, with new applications for which new legal and ethical challenges will emerge.

3. There is a risk that any response by government is tactical and piecemeal. The response will need solutions that are flexible, adaptable and non-fragile, rather than short term and rigid, and that are alert to new technologies and their uses.

4. Education remains an important part of the solution. Public education about online safety, fake news and online platforms' use of data would help users to establish community standards as well as bringing other benefits. More fundamentally, a rethink of individuals' roles and responsibilities around data is required. Ethics education for engineers and computer scientists, and more broadly everyone who handles and makes use of data, is also vital to encourage and enable responsible innovation.

5. Any regulation should ideally build on current legislative frameworks. Online behaviours are essentially digital manifestations of existing behaviours in the physical world, and it should therefore be possible to carry over from the physical to the digital domains the methods by which positive behaviours are supported and negative behaviours are discouraged.

6. Specific regulation may be needed to mandate that companies audit their processes. Many of the online platforms are currently opaque about how they moderate content, and have complete control over how it is done. Unchecked, it has the potential to be a means of censorship or suppression of free speech.

7. Online platforms dominate as a result their computing power, as well as the number of users and amount of data they hold. The investment in hardware required makes it all the more challenging for smaller companies to compete.

8. A key challenge is the global governance of the internet, and the development of a consistent global approach where common basic principles about how the internet should be used and controlled are agreed. However, there are a

number of factors that contribute to international fragmentation, including the differing value systems of world regions.

Introduction

9. The Royal Academy of Engineering welcomes the opportunity to provide evidence for the House of Lords Select Committee on Communications' inquiry on regulation of the internet. As the UK's national academy for engineering, the Academy brings together the most successful and talented engineers from across the engineering sectors for a shared purpose: to advance and promote excellence in engineering. The Academy's response has been informed by the expertise of its Fellowship, which represents the nation's best engineering researchers, innovators, entrepreneurs, and business and industry leaders.

10. As for any technology, the internet provides its users with opportunities for positive use or for misuse. The intention of its inventors was to create an 'internet for everyone'[1071] - an internet that offers organisations of any size the potential to offer services online, whether start-up or large corporate; that provides the potential for increasing human knowledge and understanding; and that enables the creation of a shared community across international boundaries.

11. The increase in fake news, hate speech, abusive messages and extremist content appearing on the internet illustrates some of the ways in which the internet is misused. For example, it seems likely that fake news is being used as a tool by state actors to influence elections and, potentially to undermine democratic consensus[1072]. Online platforms provide the vehicle for such misuses, but also rely on business models that undermine individuals' right to privacy – another type of misuse. The internet has also become a tool for cyberwarfare.

12. A central question is how to maintain values such as openness, accessibility and universality – and correspondingly, the essential attributes of the internet - while minimising the harm that misuse of the internet has the potential to inflict. The Academy welcomes this inquiry, which will inform the debate on what measures are required – both regulatory and non-regulatory – to reconcile these tensions in the most appropriate way.

An evolution in internet technologies

[1071] See for example, The Guardian (March 2017), *Tim Berners-Lee: I invented the web. Here are three things we need to change to save it*.

[1072] In January 2018, the government announced that it would establish a dedicated unit to combat disinformation by state actors and others. BBC (23 January 2018), *Government announces anti-fake news unit*, http://www.bbc.co.uk/news/uk-politics-42791218

13. A key challenge for implementing regulation or other types of measure is that the internet itself is evolving: both the underlying technologies and the ways in which they are put to use. The internet of the future will increasingly be powered by data and algorithms – as the volume and variety of data increases, and technologies such as artificial intelligence become more powerful and widely used - and correspondingly new applications will continue to present themselves over time. Legal and ethical challenges around data and algorithms will therefore also evolve. Any regulation will need to be centred around data and how it is used.

14. The volumes of data transmitted via the internet and held by data platforms is increasing, corresponding to the growth in the use of internet-connected devices – the Internet of Things (IoT). The increasing use of IoT devices in homes, workplaces and public spaces, will increase the potential for aspects of people’s lives to be observed[1073], and will generate new sources of personal data from which companies can profit. New risks to individuals’ privacy and safety are will also emerge. For example, sensors used in IoT devices allow sensitive data to be collected, through video or audio devices, or inferences may be made about individuals based on the way in which a device is used. IoT also provides a new vehicle for large-scale cyber attacks via the internet, such as the ‘Mirai botnet’ attack in 2016 that resulted in several high-profile websites being made inaccessible.

15. IoT will also increasing be adopted by industry sectors, creating many opportunities for improved performance and innovation in the supporting systems of a modern economy, generating economic value and creating social and environmental benefits across all sectors[1074]. The cyber safety and resilience of such systems is vital to ensure that they will maintain adequate levels of safety during operation in the event of a cyberattack or accidental failure, and that they are resilient if operations are disrupted. Improving the cyber safety and resilience of such systems will require stakeholders to act at scale and in a coordinated way. The global nature of the challenges necessitates global collaboration[1075].

16. The web itself provides a rich and diverse source of data. An evolution towards a web that enables its datasets to be discovered and linked, so that data could be better shared and reused, would increase the accessibility and usefulness of data held on the web[1076], and correspondingly the amount of useful knowledge that could be extracted.

[1073] Royal Academy of Engineering and PETRAS (March 2018), *Internet of Things: realising the potential of a trusted smart world*, www.raeng.org.uk/internetofthings

[1074] Royal Academy of Engineering and IET (November 2015), *Connecting data: driving productivity and innovation*, www.raeng.org.uk/connectingdatda

[1075] Royal Academy of Engineering (March 2018), *Cyber safety and resilience: strengthening the digital systems that support the modern economy*, www.raeng.org.uk/cybersafety

[1076] See for example, Hinton Lecture 2016, Professor Sir Nigel Shadbolt FREng FRS, *Engineering the future of data*, http://raeng.tv/Media/2016/Hinton-Lecture-2016-Engineering-the-Future-of-Data.aspx

17. The architecture of the internet has the potential to change too. One possible change would reverse the trend towards centralisation of data storage – instead, data would be held 'at the edge'. Currently data is held in large data centres owned by organisations, but in future it could be held by individuals in personal data stores. This would provide individuals with better control over their own data, and the ability to choose who accesses their data and how it is used[1077]. It would enable them to make more informed choices about what data they are willing to give up in return for services from third parties. It has broader benefits, such as reducing the need to transport large volumes of data over the networks, and reducing the risk of data breaches.

18. One example where consumers are being given more control over their data is open banking[1078]. Consumers will be able to decide what data they give to third parties, and for how long they give it, in order to help them make better decisions about products and services such as mortgages, loans and overdrafts. Personal data is shared between trusted organisations under controlled conditions. An open banking standard guides how open banking data is created, shared and used by its owners and those who access it[1079].

19. Any measures will need both to anticipate and respond to possible future evolutions in the technologies that underpin the internet and in the uses of the internet. For example, there could be strategic support for the development of emerging technologies that will help to create a safer and fairer internet.

What approach is needed?

20. A strategic approach would be of benefit, alongside a more direct response to the current challenges. There is a risk that any response is tactical and piecemeal, responding to received wisdoms. Instead, a more fundamental rethink is required - an important aspect of this is rethinking our approach to citizenship in a digital world, which is discussed in the section below on 'digital literacy and the digital citizen'. There is also a pressing need to address the immediate challenges around online platforms, as framed by this inquiry's questions. Any regulation will need to work alongside supporting actions such as education.

21. The future is uncertain and, in particular, the timescales over which technologies and companies will evolve is hard to predict. There may be unintended consequences to interventions. It will therefore be important to create solutions that are flexible, adaptable and non-fragile, rather than short term and rigid.

[1077] See for example, The Guardian (29 April 2018), Shadbolt, N. and Hampson, R., *Who should hold the keys to our data?* https://www.theguardian.com/commentisfree/2018/apr/29/in-charge-our-own-data-personal-information-facebook-scandal

[1078] Open Data Institute (January 2018), *Open banking: counting the steps towards a strong data infrastructure for the UK*, https://theodi.org/article/open-banking-counting-the-steps-towards-a-strong-data-infrastructure-for-the-uk/

[1079] Open Data Institute (2016), Introducing the Open Banking Standard

Ethics and diversity

22. There are critical ethical questions about the fairness of the business models used by the dominant companies. Companies have the choice about how they develop and use the technology to grow users and reap the benefits, the oversight they provide and the culture they nurture to ensure their employees act responsibly. A responsible approach to innovation is vital, but companies may be resistant to changing practices when such an approach is not aligned with business objectives. A range of ethical practices that would better benefit society are possible. For example, large search engines who manage and curate data that they have taken from the public domain could open it up and make it available for innovation by others, thus bringing wider benefit to their activities[1080]. This would not affect their core business.

23. Alternative business models for online platforms that do not rely on the exchange of personal data already exist or are emerging. For example, alternative social media platforms such as Idka or Vero rely on subscribers paying to use their services, or even pay users in cryptocurrency[1081]. Signal[1082], an open source project supported by grants and donations, provides a messaging service which does not rely on advertising and does not track its users. However these companies are tiny in comparison to the incumbents and it remains to be seen whether alternative business models will flourish.

24. Ethics must be included in the training of engineers and computer scientists, and more broadly everyone who handles and makes use of data. Ethical frameworks that support ethical behaviours should be developed and applied, building on existing ethical principles developed for professions[1083]. However, the Academy recognises that it will be a challenge to foster ethical approaches that counter the current practices of large data companies, which may also influence how emerging organisations behave[1084]. As with other technologies, the diversity of the workforce in companies developing and operating online platforms is vital, in order to create services that cater to the diversity of users.

Digital literacy and the digital citizen

25. Digital literacy should be addressed in schools, and in accessible ways – such as television, courses and websites – for adults. It is vital that individuals

[1080] Hinton Lecture 2016, Professor Sir Nigel Shadbolt FREng FRS, *Engineering the future of data*, http://raeng.tv/Media/2016/Hinton-Lecture-2016-Engineering-the-Future-of-Data.aspx

[1081] Financial Times (25 April 2018), *Are there any viable alternatives to Facebook?* https://www.ft.com/content/057fb3e8-474e-11e8-8ee8-cae73aab7ccb

[1082] Signal, www.signal.org

[1083] For example, Engineering Council and the Royal Academy of Engineering (July 2017), *Statement of ethical principles for the engineering profession*, www.raeng.org.uk/publications/reports/statement-of-ethical-principles

[1084] Royal Academy of Engineering and PETRAS (March 2018), *Internet of Things: realising the potential of a trusted smart world*, www.raeng.org.uk/internetofthings understand the personal and societal implications of entering into contracts with online platforms. Improving digital literacy must include education about online safety, but also the growing challenge of fake news and the nature of contracts between individuals and online platforms.

26. A rethink of the role of the digital citizen is needed. A new approach might consider both the rights and responsibilities of consumers, rather than solely the rights[1085]. This would help the debate on regulation of the internet, and it would also contribute to other debates such as those on automation and AI. In relation to the internet, a more active and modern view of citizenship would transform the current debate around the use of data by large monopolies such as Facebook. In an ideal situation, it should be a citizen's responsibility to manage their own data with care and thought, and involved citizens are more likely to insist on transparency and openness by powerful corporations. This would require cultural change. Education about what it means to be a digital citizen is an important aspect.

27. Furthermore, what is meant by authoritative news or a balanced argument also needs rethinking. Some information may be entirely inaccurate or unsupported, while in other cases it is the contextualisation or presentation of information that affects how it understood. Individuals would benefit from education that enables them to question critically the information that they are being offered.

Questions

Question 1: Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

28. Any regulation should ideally build on current legislative frameworks. Online behaviours are essentially digital manifestations of existing behaviours in the physical world. For example, content has always been published in the real world, as it is now online. It should therefore be possible to carry over from the physical to the digital domains the methods by which positive behaviours are supported and negative behaviours are discouraged. The practicality of implementing regulation critically depends on international collaboration. It will also be important for government and regulators to be alert to new ways in which behaviours might manifest themselves digitally.

29. For example, although online platforms are not currently considered to be the publishers of content, they might still be considered as the publishers of adverts. Therefore, they should be accountable for how adverts and other content that they have scanned and selected are displayed to users. Legislation around the improper use of postal and electronic communications

[1085] Dr John Lazar CBE FREng (April 2018), *Rebooting citizenship: responding to AI and automation*, paper for Fourth Group.

might be applicable here. Another example is that internet companies should not be permitted to examine the content of private messages - it should be an offence equal to opening someone's postal mail. If they do so then they should in addition become equally liable with the sender if the content is unlawful, because they can be held to have chosen to send the message on.

30. Any specific regulation will need to respond to the ways in which the internet is being used in practice. Often the engineering tools required to understand some aspects of its use do not yet exist. These are, however, being developed to measure activities such as third party tracking[1086] and data sharing by smartphone apps[1087]. Information about the concentration of power across third party trackers, as revealed through web measurement techniques, has only recently begun to emerge.

31. Specific regulation may be needed to mandate that companies that develop and manage online platforms audit their processes, given that these are not currently transparent and yet potentially impact their users and society more widely.

Question 2: What should the legal liability of online platforms be for the content that they host?

32. The large online platforms have evolved very rapidly and have, to date, operated with very few constraints. This is very different from the conditions in which other types of infrastructure have developed and currently operate. There is some variation between the large companies that operate online platforms about how they have expressed their intentions around fair and responsible behaviour following public and political pressure; some see this as a means of obtaining market advantage.

33. The platforms are generally attempting to resist liability for content, including the analysis of content, exploitation and onward use. However, it will be hard for them to maintain that position, and to say that they have no liability in relation to harms that result from the content, including damaging electoral fairness or in other contexts. They have, in any case, already taken on legal obligations around their terms of service.

Question 3: How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

[1086] Binns, R., Zhao, J., Van Kleek, M. and Shadbolt, N. (2018), Measuring third party tracker power across web and mobile, arXiv preprint arXiv:1802.02507

[1087] Van Kleek, M., Liccardi, I., Binns, R., Zhao, J., Weitzner, D.J. and Shadbolt, N. (2017), Better the devil you know: Exposing the data sharing practices of smartphone apps, In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. Pages 5208–5220. ACM. 2017.

34. Online platforms have put in place methods for moderating illegal or objectionable content which involve highly intensive human processes. Following the EU's privacy ruling, Google must delete inadequate or irrelevant data from its results when a member of the public requests it – again requiring the intensive involvement of humans. It is, however, only large search engine companies that have the resources to carry out this kind of activity.

35. Technical solutions are still under development, and may not completely solve the problem of removing unwanted content. For example, they may be limited in their ability to account for the context in which the content is presented, or how it is presented. Another challenge will be ensuring that the algorithms and the data upon which they are trained are not biased. Furthermore, decisions about whether to take down certain types of information may depend on a belief system or an understanding of the provenance of the content, which is difficult to ascertain with automated processes.

36. Many of the online platforms are currently opaque about how they moderate content, and have complete control over how it is done. Unchecked, it has the potential to be a means of censorship or suppression of free speech. Where appropriate, potentially stringent processes should look to the interests of individuals wishing to reverse content decisions.

37. In contrast, websites such as Wikipedia have methods for ensuring transparency engineered into their processes. They are capable of playing back the entire history of how webpages have been edited by users.

38. In certain cases processes will fall under the General Data Protection Regulation, such as algorithmic moderation based on personal data. By law, it must therefore be transparent to the user and not unlawfully discriminatory. This will be overseen by the Information Commissioners' Office.

Question 4: What role should users play in establishing and maintaining online community standards for content and behaviour?

39. There is a role for users to create codes of conduct for content and behaviour, but it cannot happen effectively without education in schools about what constitutes appropriate content and behaviour. Education about inappropriate behaviours such as cyberbullying is particularly needed, since technical solutions are likely to be less effective. Education must also teach children about how to deal with these behaviours, and there is a need for broader understanding about why children are victims.

40. As an example of a platform which involves its users in moderating content, Wikipedia has been set up as a cooperative effort with users creating content that conforms with the overarching principles that content is written from a

neutral point of view, is verifiable and does not constitute original research[1088]. It is clear about what users can and cannot say, and also allows users to continually update existing webpages. However, it is possibly more straightforward to create standards for content based on encyclopaedic knowledge than other types of content that might include fake news. Wikipedia's approach has been engineered from the outset; it is more challenging for other types of online platform to implement community standards as a means of doing this has not been engineered in.

Question 5: What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

41. Online platforms are beginning to take a role in ensuring online safety. For example Facebook has set up the Facebook Safety Advisory Board[1089], comprising internet safety organisations from around the world with which it consults on safety issues. Google is creating products to help ensure that children are protected from online harms[1090]. However, there is more that they can do.

42. In the recent past, actions to remove content by online platforms have been precipitated by commercial pressures. For example, YouTube – which is owned by Google – put in place additional moderators to take down videos that were violent, made by terrorists or inappropriately targeting children, in response to advertisers who stopped advertising on the site[1091].

43. For other types of content, the incentives for online platforms to act appropriately may not be so direct. Online platforms need to ensure that the processes they put in place to moderate content are fair and transparent, whether this is through the use of algorithms to detect certain types of content or through the use of human moderators. They will need to demonstrate this to users and policymakers.

Question 6: What information should online platforms provide to users about the use of their personal data?

44. The General Data Protection Regulation makes clear that users must be informed about the use of their personal data, including onward uses by third parties. Currently online platforms do not make this clear. At the very least, they should be compliant with data protection regulation, and the Information Commissioners' Office must have the resources necessary to enforce this.

[1088] Wikipedia: Neutral point of view, https://en.wikipedia.org/wiki/Wikipedia:Neutral_point_of_view

[1089] Facebook Help centre, What is the Facebook Safety Advisory Board and what does this board do? https://www.facebook.com/help/222332597793306/?ref=sc

[1090] Google, Family Link, https://families.google.com/familylink/

[1091] FT (5 December 2017), *YouTube hires moderators to root out inappropriate videos*, https://www.ft.com/content/080d1dd4-d92c-11e7-a039-c64b1c09b482

Question 7: In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

45. An individual affected by a decision by algorithm should have the right to transparency of the criteria, procedure and logic used to select the algorithm and determine the decision. In other words, they should have the right to know how the decision was made and satisfy themselves that it was fair.

46. Online platform business transparency should be required only to disclose practices and tools potentially harmful to or taking unfair advantage of users.

Question 8: What is the impact of the dominance of a small number of online platforms in certain online markets?

47. Business models that rely on the exchange of personal data are, at present, hugely successful – in spite of the furore over Facebook, and the greater awareness by the public about the use of personal data, companies that operate online platforms continue to profit[1092]. The activities of these companies also aim to maximise the number of users and the amount of data they hold. The acquisition of smaller companies helps them achieve this. Market domination also contributes to their success due to network effects, resulting in a considerable concentration of power.

48. A small number of the wealthiest companies such as Amazon, Apple, Facebook and Google own the largest amounts of data. The situation has the potential to create even greater disparities between individuals, countries and companies without mechanisms to keep them in check.

49. The major platform vendors may monopolise data, but there are counter examples: for example, Uber has managed to collect the traffic and map data it needs to offer its services.

50. A better form of data sharing is needed, that also complies with GDPR. Trust relies on ensuring that individual, corporate and broader social benefits from data are balanced between stakeholders. There is some evidence that the public are willing to share personal data with companies to get a better service[1093], but in many instances asymmetries still exist between organisations and consumers so that the organisation has a much better idea of how it can benefit from data than the consumer. The evolution of personal data stores (discussed in paragraph 17) is one means of countering existing practices.

[1092] FT (28 April 2018), *Big tech's stellar quarter proves the power of their platforms: Facebook, Amazon and Google earnings remain untouched by political backlash*, https://www.ft.com/content/28ad66f2-49d4-11e8-8ee8-cae73aab7ccb

[1093] A recent study of travellers' attitudes to intelligent mobility by the Transport Systems Catapult found that 57% of respondents would not mind sharing their personal data in order to get a better service.

51. The online platforms do not only dominate as a result of the number of users and amount of data that they hold; they also have huge computing power and own the largest server farms in the world to store data. It makes it all the more challenging for smaller companies to compete with the incumbents given the amount of investment in hardware that is required to compete. It has recently been reported that the tech giants are in the midst of a wave of investment that is unprecedented in scale[1094].

Question 9: What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

52. The internet was conceived of and developed as 'one internet for everyone', but there are a number of factors that contribute to its global fragmentation. One factor is language. Another important factor is the differing value systems of world regions and the corresponding controls and uses for the internet in those region[1095]. Four major regions – the US, Europe, China and Russia – can be considered here. In the US the internet is predominantly market-driven, with companies benefitting financially from the internet. In Europe, human-rights values drive strong privacy principles, and these are reflected in the EU's General Data Protection Regulation. The UK's values are closely aligned with Europe's. In the far east, China's 'Great Firewall' is used to control content that it considers to be contrary to its interests, and the internet is used for mass surveillance. Russia's attempts to use the internet in cyberwarfare are of growing concern to the UK and others[1096].

53. A key challenge is the global governance of the internet, and the development of a consistent global approach where common basic principles about how the internet should be used and controlled are agreed. This might take place in the United Nations, for example. It is vital since content may be produced and put onto the internet in different jurisdictions from its users. Without consistency across jurisdictions, companies will modify their practices accordingly to avoid controls in a particular jurisdiction. This is illustrated by Facebook's recent shifting of responsibility for all users outside the US, Canada and the EU from its international headquarters in Ireland to its main offices in California, so that users are on a site governed by US law rather than Irish law[1097]. However, the

[1094] The FT reports that Facebook plans to spend $15bn this year on data centres and other facilities, in comparison to $6.7bn last year, and Google's capital spending in the current quarter has been $7.3bn, well above its spending of $2.5bn over the last year. FT (28 April 2018), *Big tech's stellar quarter proves the power of their platforms: Facebook, Amazon and Google earnings remain untouched by political backlash.*

[1095] Talk by Professor Dame Wendy Hall DBE FREng FRS, Living in the Internet of Things conference, IET, March 2018.

[1096] NCSC press release (16 April 2018), Joint US – UK statement on malicious cyber activity carried out by Russian government, https://www.ncsc.gov.uk/news/joint-us-uk-statement-malicious-cyber-activity-carried-out-russian-government

[1097] The Guardian (April 2018), Facebook moves 1.5bn users out of reach of new European privacy law fragmentation described above makes a consistent global approach challenging.

54. The EU has the market size to hold companies the size of Facebook and Amazon to account. The UK needs to remain aligned with Europe in its approach to regulation, and to retain its influence on both European and international regulation, and ideally lead on global discussions. The UK also needs to be clear on what legal and ethical approaches should be taken that will benefit its national interests.

55. One essential attribute of the internet is 'net neutrality', meaning services do not have control over users' access to content and cannot profit from controlling access. The UK government's current position on 'net neutrality' is to be welcomed, and follows the EU's approach to net neutrality[1098]. This is in contrast to the US's approach, where a multi-tiered internet has been created following the decision in December 2017 by the US's media regulator, the Federal Communications Commission, to end the rules that protect the open internet.

May 2018

[1098] European Commission Digital Single Market – Policy, Open Internet, https://ec.europa.eu/digital-single-market/en/open-internet-net-neutrality

The Royal Society – written evidence (IRN0084)

Summary:

The Royal Society's response:

- Strongly resists a one-size fits all approach to governance of data and its uses. The internet relies on data-enabled technologies to operate. While there are governance challenges that are general in nature, many of them – and their effects – are likely to be specific. For example, the use of data to create personal recommendations for online shopping creates different forms of benefit and risk and involves different types of actors compared to the use of data in online healthcare applications. It would be a mistake to attempt to govern them in the same way.

- Calls for a renewed governance framework for data use to ensure trustworthiness and trust in the management and use of data as a whole. Central to this framework is the overarching principle of human flourishing which reflects the fundamental tenet that society does not serve data but that data should be used to serve human communities. With this overarching principle, this governance framework should be underpinned by a set of high-level principles. All systems of data governance should:

    - Protect individual and collective rights and interests.

    - Ensure that trade-offs affected by data management and data use are made transparently, accountably and inclusively.

    - Seek out good practices and learn from success and failure.

    - Enhance existing democratic governance.

- Outlines the need for a stewardship body which would be expected to conduct inclusive dialogue and expert investigation into novel questions and issues, such as those related to the internet, and to enable new ways to anticipate the future consequences of today's decisions.

- Warns against the regulation of machine learning algorithms specifically and advocates a more tailored sector specific approach to regulation.

- Outlines a series of challenges and tensions which must be considered as the capability and prevalence of data driven technologies increases including:
    - Concepts of data governance which are under strain.

- Balancing the benefits of tailored services and consumer convenience with risks to autonomy.
- Encouraging innovation while maintaining public confidence and addressing societal needs.

The Royal Society would welcome the opportunity to discuss these issues further with the Committee.

Introduction:

0.1. The Royal Society is the UK's national academy of science. It is a self-governing Fellowship of many of the world's most distinguished scientists working in academia, charities, industry and public service. Its fundamental purpose is to recognise, promote, and support excellence in science and to encourage the development and use of science for the benefit of humanity.

0.2. The Society's Data Programme is developing policy and promoting debate that helps the UK safely and rapidly realise the growing benefits of data science and digital technologies. This programme brings together leading academics, industry leaders, civil society and data and technology specialists to better understand the needs of a 21st century data governance system and the challenges associated with changes in data use and society.

0.3. In this response we highlight relevant findings from our work which are pertinent to the Committee's questions, including whether regulation of the internet is desirable or possible, transparency in the use of algorithms, and identify some additional challenges the committee may wish to consider. This draws on previous work of note:

- In 2017, the Royal Society published their report '*Machine learning: the power and promise of computers that learn by example',* setting out the potential of machine learning over the next five to ten years, and the actions necessary to allow society to benefit fully from the development of this technology.
- In 2016, the Royal Society and Ipsos Mori completed a public dialogue exercise on machine learning; gaining insights into public knowledge of, and attitudes towards, machine learning.
- In 2017, the Society collaborated with the British Academy to publish '*Data management and use: Governance in the 21st century'*; highlighting the challenge and existing tensions with data use and the needs for a 21st century governance system.

1. An evolving technological landscape

1.1. An IBM report in 2017 estimated that at the time around 90% of data in the world had been created in the last two years[1099]. Data collection activities continue to increase in speed, scale and variety, with the expansion of internet access, applications and capabilities playing a central role in this.

1.2. As the analytic techniques used to process these datasets become more sophisticated, individuals and communities are affected in new and unexpected ways. Fascinating new forms of data analysis such as machine learning have vastly increased the ability to link this data and use the patterns that emerge. Machine learning algorithms are already deployed in a range of systems or situations which shape daily life and use of the internet. Whether it be by detecting instances of credit card fraud, providing online retail recommendations, or supporting search engine functions.

1.3. Uses of data-enabled technologies promise further benefits, from improving healthcare and treatment discovery, to better managing critical infrastructure such as transport and energy. However, history has provided rich illustrations of how the widespread adoption of new technologies without effective public engagement can increase public anxiety, or result in major public controversy, both of which risk hampering potential benefits.

1.4. Further, changes to how data is used and analysed places existing data governance concepts, such as privacy, ownership and consent, under unprecedented strain. Their meanings in policy, law and public discourse have shifted, and will continue to do so in new and unpredictable ways. Uncertainties are accumulating and acting on them is necessary. However, in order to avoid long-term, cumulative and difficult-to-foresee effects, any action must be carefully considered.

2. Context is key – Avoiding a one-size-fits-all approach to data governance

2.1. The internet relies on data-enabled technologies to operate. The Royal Society strongly resists a one-size fits all approach to governance of data and its uses. While there are governance challenges that are general in nature, many of them – and their effects – are likely to be specific. For example, the use of data to create personal recommendations for online shopping creates different forms of benefit and risk and involves different types of actors compared to the use of data in online healthcare applications. It would be a mistake to attempt to govern them in the same way.

2.2. While there may be specific questions about the use of personal data and machine learning algorithms in internet based applications or platforms, these should be handled in a context-specific way, rather than via overarching regulation for all uses.

[1099] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WRL12345USEN

2.3. Practically it would be impossible and also undesirable to try to centralise data governance. Such an approach may inhibit or prevent perfectly reasonable technological developments which would enjoy public support and benefit society. In many cases there are already sector specific regulations that applications should conform to, and which are more appropriate than a one-size-fits-all approach.

2.4. The Royal Society's public dialogue on machine learning highlighted that the nature or extent of public concerns about machine learning and algorithms are linked to the application being considered. Fundamentally, the issues raised in these public dialogues related less to whether machine learning technology should be implemented, but how best to exploit it for the public good. Such judgements were made more easily in terms of specific applications, than in terms of broad, abstract principles, reinforcing the case for a context specific approach.

3. Principles for data governance in the 21st century

3.1. The internet is 'powered' by data, but this is just part of a rapidly changing and evolving data landscape, where big data technologies require us to develop new ways to use and manage data for both online and offline applications. Societies must navigate significant choices and dilemmas: they must consider who reaps the most benefit from capturing, analysing and acting on different types of data, and who bears the most risk.

3.2. While a one size-fits-all approach to data governance is undesirable, governance surrounding the use of data does require a new framework and principled approach to keep pace with the challenges in the 21st century. To ensure the extraordinary opportunities for a data enabled society are realised and that public trust is built, the Royal Society recommends two types of high level responses to data governance specifically.

3.3. First, a renewed governance framework is needed to ensure trustworthiness and trust in the management and use of data as a whole. Central to this framework is the overarching principle of human flourishing. This principle reflects the fundamental tenet that society does not serve data but that data should be used to serve human communities. With this overarching principle, this governance framework should be underpinned by a set of high-level principles. All systems of data governance should:

- Protect individual and collective rights and interests.

- Ensure that trade-offs affected by data management and data use are made transparently, accountably and inclusively.

- Seek out good practices and learn from success and failure.

- Enhance existing democratic governance.

3.4. Second, despite the range of actors already carrying out important governance functions in their specific sectors or domains, there is a clear need for a new body to steward the evolution of the data governance landscape as a whole, and to ensure human flourishing. This stewardship body would be expected to conduct inclusive dialogue and expert investigation into novel questions and issues, such as those related to the internet, and to enable new ways to anticipate the future consequences of today's decisions.

3.5. These calls were recognised in the 2017 Budget and Industrial Strategy, where the government outlined plans to create a Centre for Data Ethics and Innovation to enable and ensure safe, ethical and ground-breaking innovation in AI and data-driven technologies. The Society is pleased to see this is in line with our recommendations and welcomes the opportunity to work closely with government in this regard. The newly created Ada Lovelace Institute, established by the Nuffield Foundation to examine ethical and social issues arising from the use of data, algorithms, and artificial intelligence, will also play an important role in ensuring that new technologies can be developed in the way that public want, that exemplifies good practice, and that will allow everyone to benefit.

3.6. As the inquiry notes, there are already a number of public and private actors that regulate activity related to the internet and the use of personal data. The Information Commissioners Office considers data protection and privacy across different sectors, and actors like Ofcom regulate content from streaming services. There are also strong legal structures in place which will be built upon by the Data Protection Bill, currently making its way through Parliament, and the introduction of the General Data Protection Regulation (GDPR), protecting the processing and use of personal data.

3.7. Ensuring that these bodies work collaboratively will be key to the development and preservation of an effective governance framework which enjoys public confidence.

4. Future challenges

4.1. Many of the choices that society will need to make as data-enabled technologies become more widely adopted can be thought of as a series of pervasive tensions, which illustrate the kinds of dilemmas that society will need to navigate. As data enhances our analytical capabilities, notions such as accountability, agency, consent, privacy and ownership are becoming more difficult to maintain. Their meanings in policy, law and public discourse have shifted, and will continue to do so in new and unpredictable ways. As a result, many of the concepts that sit at the core of public confidence in governance are no longer fit for purpose.

4.2. This section outlines a series of tensions and challenges the Committee may wish to consider in the context of regulation, and how it is applied to the internet:

4.3. Existing concepts of data governance under strain. - Consent, ownership, privacy (transparency paradox)

i. Consent is one of the legal grounds for processing personally identifiable data in the current data protection regime. However, genuine consent is difficult to achieve, and is often not sufficient to ensure adequate protection of individuals' interests. First, the application of consent suffers from what is often referred to as the 'transparency paradox'. Consent requires transparency of what is being consented to. Such transparency has to be meaningful, and the mere disclosure of information is not enough. Anything too long or complex is unlikely to be broadly understood or read yet making a summary widely comprehensible often discards the details that people care about. For example, in the acceptance of terms and conditions when using internet applications or platforms. Second, it is unreasonable to expect an individual to keep track of what data is collected about them and understand how it will be used, and therefore to give meaningful, informed consent.

ii. Privacy is a deeply complicated, context-specific and multi-layered notion and its different aspects are often conflated. Data is also now often collected without explicit knowledge. It may be gathered from spheres previously thought of as private and combined with other datasets to reveal sensitive or identifiable information. The notion of privacy is also being stress-tested through the increased power of algorithms and their ability to infer and predict behaviour. The ability to draw connections between data is now so advanced that approaches to managing privacy, such as deidentification, may no longer apply. Meanwhile, the balance of risks and benefits to the citizen may play out differently in different contexts, muddying the waters with regards to what constitutes acceptable or unacceptable data use.

iii. Questions about consent are further complicated by how ownership of different data types is perceived. Data is often co-created and is capable of being silently captured, easily replicated, radically transformed, and cheaply transferred. This bears little resemblance to ownership in the way that one might own a house or a car.

4.4. Tailored public and commercial services vs risks to autonomy

i. Data-enabled technologies and machine learning applications have made it possible for users to receive a tailored online experience. For example, online music platforms can provide suggested songs or playlists, while online shops will often highlight suggested purchases based on user's previous activity. Such developments raise a question over where the line is drawn between a tailored service and a risk to an individual's autonomy.

ii. An example of where these concepts have been blurred is in the current controversy surrounding the use of data analytics in political campaigning to target specific groups or areas to the exclusion of others. The potential for personalisation comes with benefits as well as risks to autonomy. It is possible to narrowly target products and services, making it easier for an individual to seek out more suitable services and products. However, in some cases these benefits come with the risks of undesirable statistical stereotyping and profiling. This has an effect on an individual level, which could be restrictive to the way individuals engage in the world around them.

iii. It is also worth noting that statistical profiling is already in use in marketing, insurance, and assessment of threats or policing, so the need to carefully balance manages biases in data is not in itself new.

4.5. Encouraging innovation while maintain public confidence and addressing societal needs

i. Innovative uses of data offer great potential for the UK economy. It is estimated that £66[1100] billion of business and innovation opportunities could be generated through effective use of data. To keep step with the pace of change and remain competitive, innovation should be encouraged, and guided so that it addresses societal needs. However, as data-enabled technologies have increasingly large and uncertain social, economic and ethical consequences, getting the balance right will be critical.

ii. Strategic consideration should also be given to the right long-term approach to maximising value from entrepreneurial activity in this space. On the one hand, the recent acquisitions of DeepMind, VocalIQ, Swiftkey, and Magic Pony, by Google, Apple, Microsoft, and Twitter respectively, point to the success of UK start-ups in this sector. On the other, they reinforce the sense that the UK environment and investor expectations encourage the sale of technologies and technology companies before they have reached their full potential. In the case of machine learning, in order to meet the demand across industry sectors, the UK's Industrial Strategy will need to support an active machine learning sector that capitalises on

[1100] Parris S et al. 2016 Digital Catapult and productivity: A framework for productivity growth from sharing closed data. Cambridge UK: Rand Corporation. See http://www.rand.org/pubs/research_reports/RR1284.html the UK's strengths in this area and its relative international competitive advantages.

iii. With the dominance of a small number of online platforms, creating appropriate mechanisms to apportion value will be a social and technical challenge and one that needs to consider how to balance asymmetries of power between different actors and platforms.

14 May 2018

Helen Ryan, University of Winchester; Emma Nottingham, University of Winchester; Marion Oswald, University of Winchester – written evidence (IRN0018)

Written evidence to be found under Emma Nottingham, University of Wincheser

Professor Teela Sanders, University of Leicester; Dr Rosie Campbell OBE, University of Leicester; and Professor Jane Scoular, University of Strathclyde – written evidence (IRN0017)

Written evidence to be found under Dr Rosie Campbell OBE

Jenny Afia, Partner, Schillings – written evidence (IRN0032)

My Background

1. As a media lawyer and partner at Schillings – an international privacy and reputation consultancy – almost all of my cases involve online publications in one form or another.
2. I am a legal advisor to 5Rights, which campaigns to ensure all children can access the internet creatively, fearlessly and knowledgeable. I was a member of the Children Commissioner's Task Force on Children and the Internet. My colleague, Simon Brown, has helped draft this evidence.

3. Our clients tend to be extremely successful individuals, able to afford the best possible representation. Even with such advantages, it can be very difficult to prevent the dissemination of false and/or intrusive information online. We really worry what the experience must be like for those who do not have such extensive resources, particularly children.

4. The below concerns are based on our extensive experience of engaging with major online platforms when individuals have damaging and/or untrue information published about them.

Unlawful content often not removed

5. Even when English law and/or the platform’s own Terms and Conditions are on the victims’ side, content is frequently not removed. For example, in one recent case YouTube and Twitter refused to remove content advocating the genital mutilation of our client without a court order. In another case, our client was described as a terrorist in a YouTube video made by someone with an axe to grind against him. YouTube refused to remove the video despite it being false and exposing our client to significant potential harm.

Problems with Litigation

6. In such circumstances, there are limited options for escalating a complaint, save for issuing proceedings which is impractical for the vast majority of users. Having to obtain a court order is wholly disproportionate and, in effect, locks out the majority of users from obtaining effective relief.

7. For those who are willing to litigate, there are significant jurisdictional hurdles. Most of the major platforms opt for US law to govern. The First Amendment means that content that would be deemed defamatory and/or private in the United Kingdom often does not give rise to a claim in America. The SPEECH Act[1101] in effect prevents the enforcement of a defamation

[1101] The Securing the Protection of our Enduring and Established Constitutional Heritage (SPEECH) Act judgment in this jurisdiction through American courts. As a result, options for having the content removed – despite the huge harm it can cause – are limited. We appreciate the internet is global but the inability to protect people over here from content posted by people over here which causes them harm over here, is a major issue. More could be done to uphold individuals' rights in this country.

8. Particular difficulties can arise when bringing a claim against an American online platform to identify an anonymous user who has committed some form of wrongdoing.[1102] In one case we had, a client obtained a court order in this jurisdiction and yet Twitter refused to enforce it without a similar order from an American court. This creates an excessively high barrier for someone who is simply seeking to identify someone engaging in online abuse.

Practical issues when making complaints

9. Complaints, even when successful, routinely take too long to resolve. This is a major issue given the speed at which information proliferates online.

10. Most platforms do not have dedicated 'legal' email addresses where complaints can be sent to or phone numbers to speak to people. Unlike when dealing with, for example, newspapers it is extremely difficult to find a 'human' to talk to about an issue. The experience feels like dealing with a brick wall built by an algorithm.

11. There is no transparency regarding who has considered a complaint and the decision making process. This is in stark contrast to publishers/broadcasters like the BBC. The major online platforms evidently have the resources to arbitrate on complaints in a transparent. For example, a high profile client of ours was the subject of an impersonation account on Instagram. This is a clear breach of Instagram's Terms of Use, yet our complaint was repeatedly rejected and erroneously categorised as an IP complaint. It was only on the fourth occasion that the profile was finally removed.

12. Each platform requires you to use their specific online reporting tool to make a complaint, which can be difficult to use and particularly problematic if you are not a user (for example Instagram does not allow you to flag a concern about content unless you have an account).

13. Whilst successful complaints can result in a user's account being deleted, this is often inadequate as another account can be set up extremely easily using different personal details. We would like to see sites take further steps to prevent future breaches, for example blocking any accounts set up in future on the same IP address.

[1102] In England and Wales this is process is known as obtaining a Norwich Pharmacal Order

11 May 2018

Jenny Afia, Partner, Schillings and Mark Stephens CBE, Partner, Howard Kennedy LLP – oral evidence (QQ 58-70)

Transcript to be found under Howard Kennedy LLP

Professor Jane Scoular, University of Strathclyde; Dr Rosie Campbell OBE, University of Leicester; and Professor Teela Sanders, University of Leicester – written evidence (IRN0017)

Written evidence to be found under Dr Rosie Campbell OBE

Sky – written evidence (IRN0060)

Executive Summary

1. Sky welcomes the opportunity to respond to the Communications Committee inquiry. As Mark Zuckerberg put it "the question isn't "should there be regulation, or shouldn't there be?" It's "how do you do it?"[1103]

2. The growth of the large online content intermediaries in the absence of any meaningful regulatory infrastructure and inadequate enforcement has exposed society to unprecedented risks in relation to illegal and harmful content online.

3. The current model, which relies on a combination of voluntary measures and an ineffective 'notice and action' regime, is insufficient to meet demands from the public for greater accountability and more transparency.[1104]

4. It is vital that the gaps in content protection online are clearly articulated. Too often discussion gets derailed by multiple 'online' problems bundled together, which makes the challenge of 'regulating the internet' appear insurmountable.

5. This is not about regulating the internet, it is about regulating the online companies that use the internet to share content.

6. A new governance framework is needed, underpinned by statute. It should set appropriate boundaries for user protection, create standards of accountability, and allow proper oversight of companies that until now have escaped the scrutiny of traditional operators.

7. A new framework overseeing the governance of how online intermediaries develop, implement and enforce content policies and decisions need not be complicated or hard to implement, and can follow well-established regulatory principles, these would include:

    - An independent regulator established in statute with responsibility for oversight and enforcement;

    - Regulatory principles applied in a proportionate manner;

    - Regulatory powers granted in relation to:

        - Information gathering and monitoring;

[1103] https://www.wired.com/story/mark-zuckerberg-talks-to-wired-about-facebooks-privacy-problem/
[1104] http://attitudes.dotevryone.org.uk

- Creation of Codes of Practise;
- Publication of annual transparency reports with common metrics detailing effectiveness of take down processes;
- Investigation for breaches; and
- Enforcement and sanctions, including backstop power to impose financial penalties for serious non-compliance and *in extremis* the ability to direct ISPs to block sites or other ancillary service providers to withhold services.

Question 1: Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

8. A new regulatory framework that governs online content intermediaries is both necessary and achievable.

9. Recent examples such as age verification of pornography websites in the Digital Economy Act, and the wide scope of the Data Protection Bill show that regulation is possible.

10. However, internet content intermediaries themselves are not a category within the regulatory infrastructure. This means there is no sectoral oversight, making it much harder for policymakers to hold them to account for their impact on society.

11. A new regulatory category is needed to reflect online companies that profit from sharing or hosting content. It would then be possible to bring them into scope of mandatory regulation rather than rely on voluntary measures that have proved to be ill-equipped to deal with current issues.

12. A proportionate regulatory framework need not be prescriptive about the content itself but can provide much needed oversight of online intermediaries' governance arrangements. This would allow the companies to develop, implement and enforce their own content policies, but a regulator could ensure sufficient transparency, comparable reporting, and investigation for inadequate processes and enforcement.

13. It is worth highlighting that this position is consistent with the Conservative Party manifesto, which set out that:

> *"we will establish a regulatory framework in law to underpin our digital charter and to ensure that digital companies, social media platforms and content providers abide by these principles. We will issue a sanctions regime to ensure compliance, giving regulators the ability to fine or prosecute those companies that fail in their legal duties...We will also create a power in law for government to introduce an industry-wide levy from social media companies and communication service providers to support awareness and preventative activity to counter internet harms".*

14. The problem is particularly acute when it comes to offensive and harmful content. Ofcom's responsibilities are generally restricted to traditional broadcasters and, to a lesser extent, video on demand providers, but not social media companies. Not only does this create an unlevel playing field, it also means that public policy is failing to address the area where there is the most harm.

15. The UK Code of Non-broadcast Advertising and Direct & Promotional Marketing (CAP Code) is an interesting example. When it comes to the equivalent

Broadcast Code for linear TV, broadcasters are ultimately accountable to Ofcom where onerous and prescriptive rules apply. This framework means that individual broadcast channels retain responsibility for the adverts shown during breaks in programming.

16. This is in contrast to advertising on online platforms, a distinction noted by Mark Zuckerberg who recently commented "if you look at how much regulation there is around advertising on TV and print, it's just not clear why there should be less on the internet."[1105]

17. In part the reason is because of the absence of a regulatory category for online content intermediaries and lack of rules applying to them.

18. Notwithstanding the platforms derive revenue from the adverts placed, community standards do not require platform users comply with online advertising rules, and any breaches of the CAP Code bite on the uploader of the content alone. Not only are the advertising rules for online far less onerous than for traditional broadcasters but the way in which they are applied to the uploader and not the platform makes enforcement online extremely difficult.

Question 2: What should the legal liability of online platforms be for the content that they host?

19. Whilst the eCommerce Directive (2000/31/EC) needs updating, it does require that hosting providers are liable for content when they take an active role in presenting and publishing the content. This is a position confirmed by the European courts. [1106,1107]

20. It also states that hosting providers are liable if they fail to remove illegal content expeditiously once aware of it. A recent ruling in the Netherlands set this at 30 minutes in relation to infringement of copyright of live sports.[1108]

21. However, there are two key issues that emerge from the eCommerce Directive. First, it was conceived of and drafted 20 years ago in era when eCommerce looked very different. Second, it only allows for liability to be established following lengthy court procedures, meaning that enforcement is ineffective.

22. There is an urgent need to refresh the definitions in the eCommerce Directive, and with it the existing safe harbours from liability that not only have allowed

[1105] http://money.cnn.com/2018/03/22/technology/regulation-political-ads-facebook-zuckerberg/index.html

[1106] LVMH v Google France ECLI:EU:C:2010:159

[1107] L'Oreal v eBay ECLI:EU:C:2011:474

[1108] **FAPL v Ecatel ECLI:NL:RBDHA:2018:615** active hosts to grow to such an extent that they dominate the internet ecosystem, but also have led to a massive rise in illegal and harmful content proliferating their services.

23. The eCommerce legislation predated the large online companies that dominate today. For example, the categories within the Directive do not refer to social media companies or online platforms. They may be better described as a new category of 'online content intermediaries'. Instead liability regimes were created for (i) mere conduits; (ii) caching providers: and (iii) hosts.

24. While some argue that these categories still endure, particularly in relation to access providers categorised as mere conduits, they do not adequately reflect the reality of the world today with the development of highly differentiated hosting providers.

25. Whilst some hosts are passive in nature, consisting of racks of servers in data rooms, others are very much active. They publish content, encourage users to share it, and sell advertising around it. They promote some content and demote other content. They have user guidelines that go beyond the rule of law, and they moderate and remove content that breaches these guidelines. However, the distinction between hosts is not reflected on the face of the Directive, with the nuance only developed following complex legal precedent.

26. We note and support the Prime Minister's announcement at Davos on 25 January 2018, where she said:

> *"it is also right that we look at the legal liability that social media companies have for the content shared on their sites. The status quo is increasingly unsustainable as it becomes clear these platforms are no longer just passive hosts".*

27. The second issue relates to the lack of regulatory infrastructure to deal with issues of liability. The current situation, which requires courts to opine on whether liability exists for certain pieces of content, is not an effective way to deal with the challenges faced today.

28. A broader regulatory framework that oversees issues of how online intermediaries deal with illegal and harmful content would complement the eCommerce Directive. This could be done ahead of any longer-term reforms discussed above.

29. Recital 48 makes it clear that in relation to hosts, Member States can:

> *"apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal content".*

30. Article 16 also sets out that Member States shall encourage the drawing up of Codes of Content.

31. The Government should avail itself of the current provisions within the eCommerce Directive to update legislation to both impose a duty of care and to create Codes of Practice underpinned by statute.

32. In the absence of a statutory backed frameworks, including sanctions for non-compliance overseen by a new regulator, any codes of conduct produced will remain entirely voluntary meaning there are no guarantees that sufficient companies sign up, or that signatories actually abide by the terms in any codes.

33. The Government's review of liability represents an opportunity to serve as the linchpin of a new regulatory and governance framework to ensure that online content intermediaries are made accountable and responsible in managing the content published, shared and commercialised via their services.

Question 3. How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

34. Online platforms do not make transparent sufficient information, nor present it in a comparable way across the various platforms. This makes it impossible to track the levels of harm, and the effectiveness of mitigation.

35. Transparency and common reporting should be a key part of a new regulatory framework.

36. The Government's Internet Safety Strategy recognised this problem and consulted on the creation of an Annual Internet Transparency Report. It highlighted how this could be useful in benchmarking companies progress and encouraging best practice between the companies. Some the common metrics the Government considered were:

    36.1. the volume of content reported to companies, the proportion of content that has been taken down from the service, and the handling of users' complaints;

    36.2. categories of complaints received by platforms (including by groups and categories including under 18s, women, LGB&T, and on religious grounds) and volume of content taken down;

36.3. information about how each site approaches moderation and any changes in policy and resourcing.

37. It is worth considering the range of reports that Ofcom publishes in the Communication Sector. For example, Ofcom reports on customer service across broadband and Pay TV companies by publishing complaints data comparing each company on a quarterly basis. This level of comparable transparent information published by an independent regulator provides an incentive on companies to provide better service, making providers more accountable to their customers[1109.]

38. The proposals in the Internet Safety Strategy should be based on a similar model and be part of a wider Regulatory framework. A common framework for reporting should be established by a regulatory body that should be given responsibility for ensuring that information by individual companies is provided and published in a consistent way and in a timely manner. The body should set out common metrics, and use information gathering powers to ensure consistent data collection that can be presented in a comparable way. The involvement of an independent body will avoid accusations that the companies are marking their own homework.

39. It is important that users can flag content that breaches community guidelines and have a reasonable expectation that reports will be acted upon in an effective and consistent manner. Users should be kept informed about the outcome of any reports made.

40. Online Content Intermediaries should have transparent process for dealing with such reports, overseen by a new regulator. A proper process, with improved accountability will encourage users to report their concerns.

41. In the event that processes are not followed properly, users should have a path of recourse to a regulator, such as the Alternative Dispute Resolution processes that ISPs are required to have, or the role Ofcom takes in dealing with unresolved complaints to the BBC.

Question 4: What role should users play in establishing and maintaining online community standards for content and behaviour?

42. Internet companies should ensure that users can easily understand community standards, and that users are able to flag breaches, with an expectation that action will be taken.

43. The Conservative Manifesto stated that it would:

[1109] https://www.ofcom.org.uk/__data/assets/pdf_file/0013/113026/telecoms-pay-tv-complaints-q4-2017.pdf

> *"make clear the responsibility of platforms to enable the reporting of inappropriate, bullying, harmful or illegal content which take-down on a comply or explain basis".*

44. However a common complaint persists, that notwithstanding community guidelines, user reports do not result in inappropriate content being taken down, and insufficient explanation is provided as to why the reports are rejected.

45. We do not believe that platforms should rely on users to maintain standards, and as such support recent announcements of increased moderators by YouTube and Facebook, but more transparency on the nature of how platforms moderate would be welcomed and should be consistent with principles established under a new Regulatory framework.

Question 5: What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

46. Sky contributed to the Communications Committee's Inquiry – Growing Up with the Internet. We support the recommendations and believe that platforms should incorporate into their design an assumption of safety by default. In particular, we support the following recommendation:

> ***The minimum standards should require that the strictest privacy settings should be 'on' by default, geolocation should be switched off until activated, and privacy and geolocation settings must not change during either manual or automatic system upgrades.***

Question 6: What information should online platforms provide to users about the use of their personal data?

47. Recent events have highlighted how crucial data is to online platforms, and how important it is that the general public understand how this data is handled.

48. The adoption of the General Data Protection Regulation (2016/679) in April 2016 and the subsequent implementation of it via the Data Protection Bill has offered significant Parliamentary scrutiny of the way in which all companies deal with, and make information available about, personal data.

49. It is right that all companies that manage European citizen's data comply with this legislation.

Question 7: In what ways should online platforms be more transparent about their business practices - for example in their use of algorithms?

Question 8: What is the impact of the dominance of a small number of online platforms in certain online markets?

50. The emergence of large internet platforms dominant in certain parts of the market has led to increased scrutiny from policymakers.

51. In the UK, the recent BEIS Consumer Green Paper - Modernising Consumer Markets, Government proposed a new strategic steer to the CMA in relation to digital markets, stating that "new approaches may be needed….to pioneer innovative approaches to finding and solving competition and consumer problems".

52. In Australia, the Competition and Consumer Commissioner has been directed to conduct an inquiry into digital platforms, looking at the effect that digital search engines, social media platforms and other digital content aggregation platforms have on competition in media and advertising services markets.

53. In the EU, there have been consultations resulting in a proposed Recommendation aimed at "promoting fairness and transparency for business users of online intermediation services".

54. Some of the business practices highlighted by the Commission include: unexplained changes in terms and conditions without prior notice; lack of transparency related to the ranking of goods and services; unclear conditions for access to, and use of, data collected by providers; and a lack of transparency regarding favouring of providers' own competing services.

55. The Commission's proposed Regulation sets out a number of transparency measures to deal with some of the issues that emerge from the dominance of a few large online platforms namely:

    55.1. transparent Terms and Conditions through clear and unambiguous language and easily available at all stages; a notice period of at least 15 days should be given for any modifications;

    55.2. provide statement of reasons in case a provider of online intermediation services decides to suspend the provision of the service;

    55.3. transparency of the main parameters determining ranking and the reasons behind the choice;

    55.4. description in the Terms and Conditions of any differentiated treatment;

55.5. inclusion in the Terms and Conditions a description on the technical and contractual access to any personal and non-personal data, which business users or consumers provide for using the services: and

55.6. redress possibilities in the form of internal complaint mechanism.

56. The European Commission's proposed Recommendation is one of a number of outstanding dossiers in the Digital Single Market. It is important that the UK Government plays a full part in the final negotiations of these dossiers, as well as assisting in preparatory work for the new Commission. This should include preparatory work for reforming the eCommerce Directive.

Question 9. What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

57. It is often argued that due to the nature of the internet, any regulatory solutions need to be global. However, this ignores the current reality that national regulation already exists, and internet companies, like any other company, are obliged to comply with legislation in the jurisdictions in which they operate.

58. The high profile German Netzwerkdurchsetzungsgesetz ("NetzDG") law, whilst not without its critics, highlights how individual countries can have their own laws, and global internet platforms are able to comply. Even before NetzDG, local differences have existed, for example Holocaust Denial is illegal in many European Countries and because platforms such as Facebook serve local versions, they are able to comply.

59. It is clear that even within the European framework, regulatory solutions can emerge within Member States. However, the UK has also taken an active role in several important European policy initiatives in relation to platform regulation. This should continue for as long as the UK is a member of the EU.

60. That said, for historic reasons, a number of EU Member States have taken a very conservative approach to internet regulation, which has meant that progress has not been as fast as is desirable. Following the UK's departure from the European Union, it will be possible for the UK to be more progressive, and propose a bold model, that can lead the world in its thinking. This current Communication Committee Inquiry has a crucial role in helping propose that model.

May 2018

Sky, TalkTalk Group and Virgin Media – oral evidence (QQ 103-112)

Tuesday 10 July 2018

Watch the meeting

Members present: Lord Gilbert of Panteg (Chairman); Lord Allen of Kensington; Baroness Benjamin; Baroness Bonham-Carter of Yarnbury; The Lord Bishop of Chelmsford; Baroness Chisholm of Owlpen; Viscount Colville of Culross; Lord Goodlad; Lord Gordon of Strathblane; Baroness Kidron; Baroness McIntosh of Hudnall; Baroness Quin.

Evidence Session No. 12 Heard in Public Questions 103 - 112

Examination of witnesses

Daniel Butler, Head of Public Affairs and Policy, Virgin Media; Adam Kinsley, Director of Policy, Sky; Iain Wood, Director of Corporate Affairs and Regulation, TalkTalk Group.

Q103 **The Chairman:** I welcome our witnesses to this evidence session of the House of Lords inquiry into regulation of the internet. I will ask our witnesses to introduce themselves in a moment. Gentlemen, today's session is being broadcast online. A transcript will be taken. Our witnesses are from the internet service providers Sky, the TalkTalk Group and Virgin Media. You are very welcome. Can you please each introduce yourselves and, in your introductory remarks before we take questions from the Committee, tell us your view about the modern structure of the internet and whether it is currently regulated in an appropriate form? It has developed rapidly. Has regulation kept up to date with the pace of development? In your view, is it appropriate to establish a new regulatory body or perhaps an overseer of regulation? If so, what kind of powers might such a body be given or require? Mr Wood, can we start with you?

Iain Wood: I am director of corporate affairs and regulation at TalkTalk, one of the UK's major internet service providers to both consumers and businesses. We like to think of ourselves as having led a lot of the child safety debates. We were the first company to introduce parental filters and have been instrumental in some of the other industry developments since, in terms of the establishment of Internet Matters, which you might be familiar with.

To answer the question, yes, the regulatory system as it is today has been outgrown by the development of the sector. We were one of the most vocal proponents of self-regulation in the initial years of this debate. Self-regulation achieved pockets of brilliance. It achieved a lot in the early days. The development of parental filters by the ISPs and the MNOs is a good example. The way the industry, including the social media platforms, came together to support the Internet Watch Foundation is another good example. There are examples of where it worked. There are two limitations on self-regulation that have been exposed. The first is the unprecedented pace of change that you referred to. The way that platforms have gone from foundation to hundreds of millions of users, sometimes in just a couple of years, has meant that the diversity of services on offer has left consumers with a plurality of services, not necessarily understanding what policies are applied by each or what protections are in place.

The varying degrees to which companies have embraced their responsibilities is the second factor. Put simply, some companies have taken this very seriously; other companies have not and have been quite happy to hide behind the collective industry effort. Because of those two factors and given the very genuine public concern about this issue, now is the right time to look at the limitations of self-regulation and see if we can move towards a system that does not necessarily regulate away the innovation and the brilliance of the digital economy but at least puts in some ground rules that give consumers a clear understanding of what protections are in place.

Adam Kinsley: I am director of policy at Sky. I sit on the UKCCIS at as executive member and on the board of Internet Matters. Sky has had a long history of trying to keep consumers safe online as an ISP with our Sky Broadband Shield filtering tool, which is on by default, and often as a broadcaster in the online space. It is very clear to us that consumers who are using internet platforms that fall outside of the traditional regulatory spaces are not being protected. Iain talked about self-regulation—I would not even call it self-regulation. Self-regulation is usually ascribed to structures such as the ASA that come together and are independent of government. For example, for advertising, the ASA submits its decisions for judicial review. We do not have anything like that in the online space.

As Mark Zuckerberg put it, it is not about whether we regulate the internet now; it is about how we do it and probably, I would add, which companies should be in scope there. We looked at this question. We asked Mark Bunting, who is a former Ofcom regulator, at Communications Chambers. He gave evidence to this Committee at the beginning of this inquiry about whether it would be possible to create a framework. He has produced a report, which I hope you will have seen, and in which he articulates how there is quite a lot of regulation of the internet.

The social media companies—as he calls them, online content intermediaries—are taking a lot of decisions themselves. They are doing it in a very unstructured way with no oversight whatever. It is private regulation, less than self-regulation. He concludes that there is a big gap and that we urgently need an accountability framework. At the heart of it, you would have an oversight body that would have certain powers—which we can discuss—to ensure that the decisions being taken by online content intermediaries could be properly scrutinised and understood. There would be an expectation among consumers as to what was essentially happening.

The Chairman: What would be the relationship between that body and the existing regulators?

Adam Kinsley: It might well be it is an existing regulator. The report does not stipulate which institution should be responsible. The report describes the powers that the institution would have. It could be new; it could be existing.

Daniel Butler: I am head of public affairs and policy at Virgin Media. We are an ISP with around 5 million broadband subscribers in the UK. I am also on the board of directors at Internet Matters. Virgin Media also funds Internet Matters and is a funding member of the Internet Watch Foundation. I do not believe that the existing regulatory framework is inconsistent with many of the outcomes that we all want to see for internet regulation today. The founding concept that that regulatory framework was based on is the concept of safe harbour. That concept has given exemption from general liability and general monitoring for internet service providers, for hosting providers and for caching providers, but it has not excused them from liability to take action where they are aware of illegal content across their services and platforms. That framework has been sufficiently flexible to give rise to a wide variety of co-regulatory and self-regulatory initiatives that have increasing efficacy. We are now seeing models come forward in which a very proactive approach to the filtering out of harmful content is being undertaken right across the spectrum from ISPs and how we deal with copyright infringing material and child abuse material to search engines and social media platforms which are applying technological innovation to how they approach content moderation.

Iain points to a couple of limitations in the existing outcomes that we see from that framework. I would not disagree with his comments, but I would reframe them and say those limitations are, for me, not foundational. They do not prove that the existing framework acts as a constraint to these initiatives emerging. They are uneven in their outcomes, which is something we should solve for. Broadly speaking, the proposals that have come forward sponsored by Sky are addressable within the existing legal construct.

As a final point, there are good reasons why that legal framework was designed in the way it was. It was designed to give rise to competition and as an acknowledgment of the decentralised nature of the internet and the importance of free expression on the internet.

Lord Gordon of Strathblane: I have a supplementary point to ask Mr Butler. You said that the degree of self-regulation is uneven. How are we going to even it up? Does that not imply an external intervention?

Daniel Butler: Sir, there are merits in some of the ideas that are coming forward for a new regulator or a new body that can do a couple of things to support additional efforts in internet regulation. Transparency reporting can act as a soft incentive for smaller companies, in particular, to, colloquially, up their game in internet regulation. There are some incentives that you could envisage a new regulatory body having that would encourage the long tail, if you like, of smaller platforms to invest in new ways of content moderation. My broader point is I do not think you have to start again, in terms of the legal framework that exists within the e-commerce directive that has given rise to a thriving digital economy, in order to achieve those things. There is a middle ground in which a new set of standards codified in regulation could be helpful but perhaps not as transformative as politicians might expect.

Lord Gordon of Strathblane: It seems to me that we might need legislation of some kind to give whatever external regulator there might be the power to exercise this influence, however gently, on the various companies. Would you be opposed to that?

Daniel Butler: Opposed to new legislation?

Lord Gordon of Strathblane: To create a light touch regulator, but somebody has to drive the action.

Daniel Butler: No, I would not be opposed to a new statutory framework. I would see it as a partial response to the bigger societal question that I would love to explore during this session. The creation of a new regulator with specific powers inevitably takes you towards the process and technical end of interventions, which is important but partial. It is a partial response to our objective of creating a safer online environment.

Q104 **Lord Goodlad:** What assessment have you each made of the Government's response to the consultation on the Internet Safety Strategy?

Adam Kinsley: It is interesting. It is typical of the policy responses in this space so far, which have been quite narrow in scope. There has been a lot of noise about certain activities, and there is a governmental response to that. For example, the code of conduct that the Government have put forward does a number of things. A mantra coming out of the department is, "What is illegal offline should be illegal online", yet the code only deals with legal content.

DCMS and the Home Office have said, "We will look at this much more holistically", but the code does not do that yet. It is perhaps too narrow in scope. It talks about social media companies, which has not been defined, and that may not be broad enough. It does not mention, for example, some of the techniques where the platforms are using algorithms and AI. It feels like it is relatively narrow and we will probably need another code to do other bits of the equation. That is why we think the right answer is that an independent body is created that can look at the harms, assess them based on evidence and come up with a proportionate framework that deals with this in a much more holistic, measured and consultative way with the companies involved, assessing the harm and working with civil society. It is a good example of a relatively narrow intervention that they have probably done quite well, but it is too narrow and it has probably been done, if I may be so bold, by the wrong people.

Daniel Butler: I thought the Government's response was, in some ways, a fair reflection of the commitment and the effort and the incentives that exist for internet companies to undertake activity to make the internet a safer environment. I was grateful for the recognition that the impact of things such as Internet Matters got in that response. In general, I was left feeling that this was a missed opportunity for Government to set a longer term set of strategic goals for online safety. Some of the evidence gaps that were acknowledged in the literature review that UKCCIS did to support the Green Paper were ignored by government.

Those evidence gaps present more fundamental questions to government about online safety that are somewhat removed from the low-hanging fruit of a new round of technical interventions. Generally speaking, we have been on the merry-go-round of technical interventions for too long without giving due regard to the broader societal challenges and interventions that are required to equip young people to get more out of a safer online environment. In particular, that literature review acknowledged that we do not understand the causal relationship between a young person seeing online harm and what that does to them in terms of their motivation to act. If we are designing frameworks that are to enable young people to be more resilient and to navigate this world where we acknowledge we cannot sanitise it completely, then the Government, sooner or later, need to grip that challenge and think, "Well, how do we better equip young people to navigate this world"?

Iain Wood: We spent a lot of time talking to Ministers and the officials at DCMS about it and I welcomed their very genuine desire to get this right. The question is whether the Government's response is sufficiently radical to deliver the improvements that Ministers and officials want to see. Things like the code of conduct and transparency reporting are welcome initiatives. I worry that if they are done on a voluntary basis, they simply will not deliver the improvement necessary. One of the biggest problems I see is the disparity between the ways different companies treat this. A voluntary code of practice and a voluntary transparency report, although well intentioned, risk exacerbating that problem. Some companies—probably the large ones—in the public eye will sign up to that. Other companies will not. Rather than removing the variants we see, we end up entrenching them. There are good ideas there, but I would be inclined to go much further and to do it on a statutory basis.

On the issue about the strategy versus a series of tactical options, one example where I would have liked to have seen more strategy in the document is around the role government can play in marshalling the sorts of initiatives that the private and charitable sector support. The problem is not necessarily a lack of will or a lack of money. In some cases we have it. What is lacking is sometimes a coherent plan. To take one concrete example, in terms of the support available for parents online—we know lots of parents feel confused by this and want access to good reliable advice—there are so many duplicating initiatives often done by individual charities or individual companies which are protecting their policy on their initiative at the expense of coming together and collaborating and saying, "What are one or two sensible scalable options here that can materially move the dial, and we will all collaborate to put our resources behind those?" There is a genuine role for Government in forcing that debate. I worry that left to their own devices, everybody will continue to run their own little programme, which, although well intentioned, collectively ends up being less than the sum of its parts.

Adam Kinsley: Can I add to what Iain said? First of all, I agree with that last point, which was well made. In terms of codes of conduct, I sit in various different fora, particularly in Brussels, where there are lots of different working groups and lots of different codes are established. They spend ages writing the code. It is agreed. Typically a commissioner will hold up a piece of paper. That is the end of it. There is no creation of a framework of what effective action will happen. There is no monitoring of what then subsequently happened. There is no reporting back on what happened, apart from one or two very rare deviations from that that I can think of. Generally speaking, the code is published and that is the end of it. That is what I fear is lacking here. There needs to be a way of measuring the impacts of any of those interventions. Another role we see for this oversight body is some aggregate reporting of progress.

Q105 **Baroness Quin:** I want to pick up on what you have just said. You are all saying, in slightly different ways, there should be strategic goals for online safety and an overall plan. Is there a consensus as to what those goals should be? Is the problem that they have not been organised or implemented in an effective way? What should the next step be in terms of the strategic goals and the plan?

Adam Kinsley: My sense is there is more of a consensus about the need to create an evidence-based organisation, or to empower a body to do exactly that job. I do not think we know the answer to that question as to what are the strategic goals that we are trying to solve here. We do it at a very high level, but I do not think the evidence base necessarily sits in one place to map out what the right policy goals are. That is why we think that that needs to be done. There is a consensus that it would be best done by a body that is empowered to do that and can think about these things in a very evidence-based way. I am not sure we necessarily do know the answer to that question.

Baroness Quin: Is it a British body, a European body or a world body even?

Adam Kinsley: At this stage, it is bite-sized chunks and what you can achieve. Certainly, there is scope to do this in the UK. I agree with what Dan was saying earlier. You do not have to rip up the e-commerce directive to do any of this stuff. It articulates back from 2000 the concept of a hosting provider. Case law has then been used regarding active hosts and passive hosts. This idea that there are active hosts that are curating information, selecting information, prioritising some and deprioritising others—that exists. The e-commerce directive recognises, with regards to illegal content, that member states can impose a duty of care here so that hosts meet their legal requirements. We do not have to rip up any European frameworks. We can do this—the Germans have done it. We can do it as well and we can show what best practice looks like.

Daniel Butler: We fell into the trap there, Baroness Quin, of fixating on one form of technical intervention and one model of regulation. For me, the missed opportunity is that the Green Paper failed to look beyond those technical interventions in the debate that this Committee has provoked. I think that from this point we will find it relatively easy to find consensus on some of the technical and regulatory design questions that the Committee is grappling with.

The bigger issue, which government have not shown any appetite to address, is that there is evidence to suggest that because the nature of harm has evolved on the internet from a relatively contained content risk to risk associated with conduct and contact, the holistic solution is to equip young people to recognise risk and to develop their strategies for navigating it. It is called digital resilience. It has become a somewhat vacuous and hackneyed phrase because there has been a lack of research and government willingness to really understand what digital resilience is, what it looks like at different developmental stages and how we build it. We have undertaken some research on that primary question. The initial results that have come back show that we do not have a good view of what builds digital resilience today, but we know that the thing that diminishes it is turning off the device, removing children from the internet and preventing them participating in that world.

Baroness Kidron: I will put on the record that I know all these gentlemen outside of the Committee. Dan, I agree with a lot of what you said about not blocking and not stopping, and so on, but I absolutely have to ask you this question. Is it the duty of children to adapt to the commercial needs of the digital environment? Is it not the duty of the digital environment to adapt its commercial needs to those of childhood and children? In asking the question, I would specifically ask you to point to any other industry that is allowed to have even causal effect or causal harm on children—forget about the evidence base—that we would allow. I suppose you could point to the food industry, maybe, if you eat badly. I have to ask you that question.

Daniel Butler: It is absolutely the case that private actors have responsibilities. Each of us, as private actors, has shown willingness and responsibility beyond any commercial incentives that we may have. That is clearly demonstrated. Ultimately, the relationship that matters here is between the parent and the child. Our primary research with the Oxford Internet Institute demonstrates that. The one condition that seems to generate more resilience is a digitally aware, digitally skilled parent who can have an active parental role in their children's online life. That is the fundamental relationship. I am not suggesting that children should be out there without any rules of the road or without any support from either private actors or their parents. Those conditions are absolutely necessary to be present. We need a realistic view that because of the nature of online harm, there will be situations in which the child encounters harm completely on their own. I would not want to be advocating a policy that was not at least looking to address how we can better equip children when they are in that situation.

Iain Wood: There are three buckets to this question; there is the product bucket, the parent bucket and the child bucket. There is a moral obligation on providers to make sure that we are providing a service in a way that protects children. That means walled garden content; it means parental filters. We are trying to make sure that we are providing it in a way that minimises the child accidentally stumbling across anything they should not and coming into harm. That is point 1, and that is how we have designed the product.

The second bucket is how we help parents understand and mitigate online risks. A lot of parents will say, "I don't know what's appropriate for them to be looking at. I've heard of these social media websites and platforms. I don't know if they should be on them. What's appropriate for a 13 year-old?" What is appropriate for one 13 year-old is not necessarily appropriate for another. There is an information element that we have an obligation to help with to make sure that parents are able to make informed choices about how to protect their children.

Having done those two steps, the remaining issue is how we equip children to deal with online harms. As Dan says, even though you try to avoid them coming into contact with harm, we cannot remove all risk, just as we cannot remove all risk from children in the physical world, in the same way that if you send a child to a park, you put in place precautions and try to minimise the risk but you cannot be 100% sure that they will not encounter any. As Dan says, there is a backstop that we have to think carefully about, which is digital resilience. Ideally, they never encounter the risk in the first place, but if they do, there is something there to help them.

Baroness McIntosh of Hudnall: I want to pick up on Baroness Kidron's point. If I were going to be very disobliging, I would have to say these arguments sound remarkably self-serving. I do not want to be offensive, but that is how they appear, to me at least, because the point that all of you have made—and particularly, Mr Butler, you have made this point very reasonably—is that the speed at which these opportunities to participate are evolving is very hard to get ahead of. We all understand that. In a way, we must manage that reality, must we not? We cannot say, "Well, that's the way it is, so everybody else will have to get up to speed", and particularly not with children.

To take the park analogy, which I completely understand, we cannot protect children from harm but we do not expect the park to be different every time they go there. There must be some way in which there is some kind of intervention that is not just about saying to kids, "Watch out. There could be dangers", and saying, "The dangers will be different the next time you go there". How do you build that into a system that relies on the child and the child's parent to be the mediators?

Iain Wood: Perhaps I have not expressed myself as clearly as I could. I am not suggesting at all that it is the responsibility of the child or the parent to protect themselves. If you take the core service that we provide, the internet, into someone's home, I would argue the core responsibility and the moral obligation sits with us to try to provide that in a way that protects the child. In our case, it is the parental filter. You cannot sign up for a TalkTalk service without making an active choice about whether you apply the filter. The default is to apply it. If you apply it, there are nine categories. We have pre-ticked six that we think are inappropriate for any child. These are things such as dating, gambling and pornography. There are a further three categories that are not necessarily inappropriate for a child but some parents might want to restrict—things such gaming and social media. That provides the internet in a safe way.

It is a technology solution, and no technology solution is perfect. It works on key terms. Sometimes it might underblock; sometimes it might overblock. Therefore, the next stage is the parental stage, helping parents understand how to apply that and understand that. The final stage is helping children understand the risks online because no technology solution is perfect. It cannot be a completely safe area. You have to equip the child with that knowledge. It is about supporting the child; it is not about removing the obligation on the provider to provide the product in a safe way—absolutely not. That is the first part of the building block, but all three of those have to come together.

Adam Kinsley: In terms of this inquiry, which is to do with regulation of the internet, that is the first bucket—the companies. We would like to think we are all responsible—companies are all regulated in the UK, there is a structure and there is a framework. We are called in by Ministers. We turn up because that is what you have to do. We have a different situation with large global platforms that may have designed their products without necessarily thinking about the most vulnerable use case. That might be a different scenario to how we might think about a product where we are putting safety by design right in at the beginning. That is the nub of it. I agree that you need to have a way of ensuring that that first bucket, which is the companies, acts responsibly. All the evidence suggests that that has not been happening. It is because there is not a regulatory framework requiring them to do so.

Baroness Benjamin: You talked about parents and their responsibility. Who should be educating the parents? There are many parents out there who do not have a clue. All three of you have said it is the parents' responsibility. There are some parents who do not know how to work the computer and do not care about what their children do, et cetera. How do we get parents to take up the responsibility? Who will teach them about what to look for when they navigate the internet?

Iain Wood: That was the exact problem we faced in 2014 when we established Internet Matters. At that stage, I think we had all launched—TalkTalk certainly had—our parental filters, which provided a safe gateway to the internet. When we heard back from parents, they were saying, "It's great that you have this free tool. It's great that you're offering it, but we don't necessarily understand how to use it". As I was saying a moment ago, we do not necessarily understand what risks there are online or what is appropriate or how to use these tools. That is why the four major ISPs came together to launch Internet Matters. It is a dedicated not-for-profit directly targeting parents, not to tell them what to do or what not to do but to offer them a range of helpful information so that they can make an informed choice about what is right for their home. We felt we all had a moral obligation to support Internet Matters and to help offer that. It has been hugely successful. We are very proud of what it has been able to achieve. One of the things we would like to see come out of this whole debate is more companies supporting Internet Matters with financial contributions so it can reach more parents than it already does.

The Chairman: Baroness Benjamin referred to, in effect, some issues that came through from our previous inquiry on children and the internet. We found that there was very, very good practice across the industry with Internet Matters and a number of other bodies doing a lot of work with children and parents. However, there was a lack of co-ordination and, if not conflicting programmes, a lot of small programmes trying to achieve the same thing somewhat inefficiently. Is that being addressed? Is that improving?

Adam Kinsley: No.

Iain Wood: No.

The Chairman: No.

Iain Wood: The point of Internet matters was to address that. We were all running various different initiatives to support parents. When we spoke to each other, we realised that between the four major ISPs, we were in 90% of homes in the UK. We said, "If we co-ordinate our efforts, combine our efforts and pool our resources, we can reach so many more parents and be so much more effective". We launched it as a four but the hope and aspiration was always that over time, a range of different companies across the sector, including social media platforms and device manufacturers, for instance, would join Internet Matters and it could become the industry body that combined those efforts and reached parents in a much more consistent way.

The Chairman: Is there anything the Government can do to nudge in that direction?

Daniel Butler: Government, in their response to the initial proposal of a social media levy in the *Internet Safety* Green Paper, acknowledged that the charitable sector's response was lukewarm at best. To characterise their response to it, it seemed to be the concern that this would give rise to a more disparate advice-giving community and that was not in the strategic interests of any single advice-giving organisation today. There was a recognition that it was not conducive to better outcomes either. We know from Internet Matters that you need strong brand recognition and a one-stop shop if you want material numbers of parents to engage in your platform again and again. Through Internet Matters, we advocated that that was the right model. There was general concern that the levy would make for a more disparate environment.

Adam Kinsley: The features of something such as Internet Matters, which has a number of companies all contributing and dedicated staff who are pushing out information, making it current and live, are right. When we set it up, Sky had its own online safety advice centre that we tried to manage. It was probably okay but it was not the best because it was not current enough. It was always a little bit behind. These guys were doing the same thing. At some point, we had to put our corporate branding and just cut it and say, "We're not going to do that. We're going to hand it over to another organisation". The Royal Foundation, another forum that Baroness Kidron is on, wants to create a sustainable model to deal with cyberbullying. If we could come together with the collective, we would be prepared to say from our perspective, "These are the features of the organisation. It needs to be done centrally. Someone needs to convene this and push industry together. We do not mind what the name is, but we think we can do more than the sum of the disparate parts".

The Chairman: Is this a typical charity sector problem? You all talk about what industry can do to put resource and support into a single organisation, and pool your own expertise, talent and resources, but are there too many competing organisations, bodies, charities, all trying to do the right thing, that ought to be folding into it at the other end?

Iain Wood: I was trying to tiptoe around it diplomatically earlier. To answer your question, yes, that is precisely the problem.

Baroness Kidron: Or is the Government not doing enough?

The Chairman: Can the Government nudge?

Iain Wood: It is a difficult conversation for government to force, because invariably there will be winners and losers. The losers will be very noisy. I understand why Ministers might be reticent to force that conversation, but if we are genuine about this, then I think we have to.

Baroness Quin: My question, in a way, continues the theme of the responsibility of private actors. It is about the role that platforms and intermediaries can or should play in policing online content and behaviour. There has been debate about this in the context of the copyright bits of the digital single market directive, and so on. Is it reasonable for intermediaries to play a more active role in policing online content behaviour? If so, who should bear the costs of building and maintaining the systems and technologies required to do so?

Adam Kinsley: When you are talking about internet companies, you have to be careful about which ones you are talking about. In my mind, that question is about the active hosts, doing stuff with the content—arranging it, promoting it and demoting it. The company has terms and conditions that it tries to apply; it has its own private rules. The idea that the online content intermediaries are passive and are not doing anything is wrong. They are. Facebook described itself as a publisher in a lawsuit in the US last week. They have said they are not just platforms. They are somewhere in between. That is right. They are doing a lot in some areas. They are using lots of moderators—both Google and Facebook have talked about 20,000. They are using a lot of AI. They are taking down a lot of content.

If you have a platform where there is an editorial responsibility, because there are terms of use, you have a duty to police it. That cost goes on those companies, which is right and proper. The debate is often mischaracterised, very much so in the copyright directive, which has gone through a very bruising encounter, as my colleagues in Brussels tell me—I was there on Friday. There was a massive campaign and I am not sure who was paying for it all but I have my suspicions. At the heart of it, for copyright content, a company like Sky that owns a lot of rights finds its content appearing on online platforms. A company like YouTube has lots of content. YouTube has a very good tool called Content ID. What that means is if we notify them that some of our content is on their platform, it gets taken down. Because we have given them the metadata, it does not reappear.

All the copyright directive is saying is to have that obligation set out in the directive and require that of other platforms that do not do that. It is not going to break the internet—at least it was not the last time I checked YouTube. The campaign, just to illustrate, is that there are exceptions in that directive. One is to do with online encyclopaedias. Yet, in certain member states, Wikipedia blacked itself out as a protest. It is not even in scope. There is a lot of misinformation. We spend a lot of money trying to protect our content and investing in the systems to detect it on the platforms. They have a duty to police their terms and conditions. That is a fair compact.

The Chairman: Do you have less of an interest in content?

Daniel Butler: An increasing interest, but, historically, yes. Copyright is a germane area to focus this question on because industry’s response to copyright-infringing content has gone through quite an evolution within the existing constraints of the e-commerce directive. ISPs were the first actors required to take notice-and-takedown steps against copyright infringing websites under the 97A court order provisions of the Copyright, Designs and Patents Act.

We have taken action against The Pirate Bay, Newsbin and some of the prominent peer-to-peer copyright-infringing websites. That activity started in 2011 and continues to this day. It evolves on a monthly basis, when a new block list comes from the BPI, the Premier League and the MPA. In addition, in more recent years we have seen search engines required to undertake legal or takedown action against copyright-infringing websites, including deprioritising them in search results. The private sector, YouTube, evolved their Content ID system to respond to copyright-infringing materials. As a result of a dynamic court order our own approach has evolved and we now intercept live copyright-infringing broadcasts of Premier League and UEFA content. That framework emerged in 2017.

That all occurred within the general safe harbour exemptions described at the outset of the e-commerce directive. I am not as familiar with current machinations of the revised copyright directive, but when that was going through the European Parliament one of the early concerns was that in moving to a notice-and-staydown approach it was difficult to see how it would be compatible with our existing framework. In order to ensure that something stays down it implies a general monitoring obligation on the platform or internet service provider. In dealing with copyright-infringing material, the e-commerce directive has enabled a great deal of innovation and efficacious approaches from private sector companies.

The Chairman: Do you agree, Mr Wood?

Iain Wood: It is possibly helpful in this debate to consider the responsibility of a platform to separate copyright out, because it is quite a distinct issue compared to other issues such as harmful content. Those are separate things. Clearly the debate has moved on. It is not a question of whether the platforms have an obligation to monitor and police content they host. I would hope everybody is of the view that they do have an obligation. The question is merely, "How?"

The key question is whether we want to allow such flexibility that any platform can choose how they do that and it is accepted there is a diverse approach, in which consumers may be unsure as to whether they are protected or not, or whether we want to set some basic ground rules. I am firmly coming to the view that some basic ground rules should be set so consumers are confident of what protections are in place.

Lord Gordon of Strathblane: Is this a self-defining exercise? Does a platform itself decide it is passive or are there objective criteria that can be used? As a layman, even the most passive seems to be quite active when it comes to controlling advertising revenue

Adam Kinsley: You are either active or passive. When considering passive hosting providers I have in mind cyberlockers, or servers in data rooms that are hosting providers but are not profiting from the distribution of the content. There are no financial incentives for ordering content in a certain way. The ones that you have in mind are probably active, as defined by European case law and the case between L'Oréal and eBay, in which the concept was discussed. The platforms you have in mind are the new versions of hosting providers that emerged post-2000 that are arranging, suppressing, selecting and promoting content and profiting from that.

Q106 **Viscount Colville of Culross:** I declare an interest as a TV series producer. Do you all accept that liability is shifting, with online platforms increasingly accepting more liability? Mr Kinsley, you spoke in your submission about the need to refresh the definitions in the e-commerce directive, which sounds interesting. What does that mean? How does that turn into changing the liability? Mr Wood, you spoke of whether ground rules were needed. What would such ground rules be? Mr Butler, you appear more concerned about the role of strict liability and the difficulties for platforms in policing such a thing.

Adam Kinsley: There are emerging pieces of legislation and proposals from Brussels that recognise the bluntness of the e-commerce directive and the fact that hosting providers since 2000 have developed. In European case law there are now active hosts and passive hosts. In the long run, given some of the proposals in the copyright directive recognising that active hosts are doing monitoring and regulating their own platforms, the idea there should be no monitoring whatever is already outdated. There is another recommendation in Brussels for the treatment of illegal online activity where the Commission is very clear there should be active, pre-emptive activity by the platforms.

In the long run, perhaps in the next Commission, there ought to be a way of breaking out hosting providers into a more granular model. However, in the short term that is unnecessary. The ideas discussed here are perfectly commensurate with the existing directive. It is about recognising that the platforms already police content to differing extents, but there is no accountability as to what they are doing. For example, how are they doing it? What is the split between moderators and AI? How are they doing it across different content classes? What does it look like when they are considering reports from children?

None of that is transparent. Transparency is only available when the platforms decide to do it, on a global basis, at a time of their choosing. We need to move away from that. To answer the question about where online harms exist, regulators and policymakers need to understand what is happening. At the moment we do not have that insight.

Iain Wood: When discussing ground rules I am referring to what I consider the basics. It is not an attempt to have a catch-all piece of legislation that covers every aspect of the debate today. It is the basics, such as default privacy settings and what they are. For example, are there separate default privacy settings for children? How do platforms handle complaints about content? What is the SLA on any particular complaint? How often is the complaint upheld? All those basic things could form a basic set of ground rules. To be clear, it is a floor and not a ceiling. A platform is in no way prevented from going beyond those ground rules, either because the platform has higher standards or because there is commercial benefit in going above that. It would provide a floor and a consistency of approach so consumers can understand the protections that are in place and make informed choices about whether they use those platforms or not.

Daniel Butler: The liability question is somewhat removed from the discussion we have just had, which, as Adam characterises it, is an approach that exists within the current liability construct. In our submission we imagined a world in which we depart from the consensus position of today and envisage something much more strict in relation to the liability and obligations on platforms. We pointed to some potential negative unintended consequences and externalities that could flow from that, the primary one being false positives.

Looking at the German regulation, their companies are required to very quickly assess a very high volume of content on subjective grounds, not necessarily legal or illegal grounds. There is a grey area of harmful, leading to extremist material that they must quickly evaluate. If they get that wrong they face material fines. What behaviour does that institute? It institutes a conservative behaviour on the part of the platform and risk aversion to allowing content on the platform, which ultimately generates a high degree of false positives. It has consequences for free expression. Ultimately, taken to its extreme, it would alter the character of the internet.

Those are questions for parliamentarians to grapple with, because that is a trade-off. One does not want private companies making the judgment whether the potential negative harm to society of a piece of extremism material slipping through the net is worth that cost.

The Lord Bishop of Chelmsford: Why is that a problem? If there was some sort of appeal process, I do not see why that would be a problem.

Daniel Butler: That becomes a question of what period of time is acceptable to constrain someone’s free expression.

The Lord Bishop of Chelmsford: Yes, but why should the appeal always work the other way? The people who are affected by the harmful content have to appeal to take it down rather than the other way around.

Lord Gordon of Strathblane: The same thing happens with newspapers, which make a decision whether publishing something is in the public interest or not.

Viscount Colville of Culross: Yes.

Daniel Butler: I do not have any particular response to that. It is a fair challenge. I am not saying that—

The Lord Bishop of Chelmsford: What do you think?

Daniel Butler: There is an extreme version that does not look very attractive for a liberal society. There is then a model with appeals processes, with perhaps some lower constraints on the platform that involves less of a trade-off with free expression. Ultimately there is a trade-off and it is a debate for Parliament to have.

The Chairman: What does the extreme version look like?

Daniel Butler: The extreme version is the one I described at the outset: private companies effectively making risk-averse decisions that alter the average citizen's ability to upload content.

Baroness Kidron: Is that not an argument for oversight of societal issues?

Daniel Butler: That is right.

Baroness Kidron: I agree with you that it is not the job of private companies to determine what constitutes hate speech. That is something we have to come to together and we all may be unhappy with where we come to. Is it not an argument for having some societal answer to the liability question, rather than a very narrow piece of legislation that pushes it back into the private arena?

The Chairman: You all hinted at that in your opening remarks.

Adam Kinsley: I want to add to that. I agree that, because of the problem you defined, that is exactly why oversight is needed. It is not fair on the companies, to be honest. The risk that Dan highlights does not only arise because of the German law. Platforms are taking down hundreds of thousands and millions of accounts. Twitter announced yesterday that it is approximately a million per day.

Baroness Kidron: Yes.

Adam Kinsley: They are doing this anyway, even without a NetzDG law. It is not because of the law that they are doing it. They are doing it anyway, but they are doing it with no accountability. I absolutely agree with you, Baroness Kidron.

Iain Wood: Adding to that, there is a debate about filtering versus blocking and how we try to bridge that divide at the moment. It is not appropriate, given that the four major providers cover 90% of homes in the UK, that between us we could get together with our counterpart from BT and essentially decide to shut down a bit of the internet because we do not think it is appropriate. It is not our place to make that judgment call. We can offer tools to customers so that they can choose to filter things they do not want to see in their home, be it pornography, gambling or violence. What we block at a network level, with the customer having no choice whatsoever, should be decided by Parliament. Anything that is illegal, we will of course block. That distinction is an important one, because in trying to protect children, which we all want to do, we have to remember that while there are some niche parts of the internet that not everybody in this Committee room would like to visit, a consenting adult does have a right to access it if it is legal content. We are trying to strike that right balance.

Adam Kinsley: I disagree. I fundamentally disagree with that. If you are a private company such as Facebook and you decide that you do not want nudity on your platform—which is perfectly legal—it is within your right to do that. I often discuss the Matt Hancock app and his rules of engagement, but perhaps that is irrelevant now. I frequent a bulletin board site for supporters of Tottenham Hotspur.

Baroness Kidron: Sad.

Adam Kinsley: It has a filter for swearing and completely censors what I write. I will not say the phrase I might want to say, but what it would turn it into is, "I naffing love Harry Kane". It might not be what I put in, but that is how it comes out. It has a swear filter. It completely censors what I am saying and it makes for a really nice environment. It is up to companies to decide whether they want to do that.

The Chairman: What is wrong with that, Mr Wood?

Iain Wood: We are comparing apples and pears. One is about a service such as Facebook or Snapchat that a customer has decided to access and in that instance it is absolutely correct that the provider sets the rules, just as something in the physical world, such as Tesco, can decide what is allowed in its shops. As an internet service provider, what we are providing is not something that the customer has opted into, which is just access to the internet. We have to be very careful not to shut down things, due to our net neutrality obligations. Customers must be able to access legal content. We are comparing two very different things.

Adam Kinsley: Now I agree with you.

The Chairman: Right. You accept that distinction.

Viscount Colville of Culross: Mr Kinsley, you discussed the need for transparency and, Mr Wood, you talked about setting very basic ground rules. We have discussed the difficulties, or the benefits, of private companies doing that, but should we set up some sort of regulator to oversee it, that will bring in all these societal obligations and set these ground rules and the transparency?

Adam Kinsley: I think so. To examine some analogies, we are all regulated by Ofcom. We must all submit to information requests from Ofcom. If we do not, Ofcom fines us. With that information, it then undertakes an assessment of harms and risks in the market. On a quarterly basis it publishes information about complaints that we receive. We compete very, very vigorously to ensure we are not at the wrong end of that list and improve our performance as a result of it. I see that analogy being taken into this space. I have no doubt whatever that their performance would improve if you shone a light on it.

Iain Wood: I agree. Start from the premise of what problem are we trying to solve and then work back to what the regulator looks like. But we will probably get to the end point that there needs to be regulation of this. It can either be a new regulator or it could be extending the remit and probably the resources of an existing one like Ofcom. I do think it is necessary, precisely to underpin those ground rules that we talked about earlier. The telecoms analogy is apt here because, although TalkTalk is a UK company, most of our rivals we compete against are big international companies. They exist in Europe, where there is pan-European legislation in parts. They compete in countries around the world that European legislation does not extend to. They also operate under UK-specific legislation and regulation that Ofcom applies.

There are clear instances of the large companies that I am sat next to operating with country-specific regulation. I do not buy the argument that simply because you operate globally there somehow cannot be UK-specific standards. It is of course easier to operate where there is regulatory alignment across different jurisdictions, but it does not mean it is impossible if there is not.

Viscount Colville of Culross: What is your objection to that, Mr Butler?

Daniel Butler: I do not think I have an objection. I would say that one should be clear about what additionality one expects from a new regulatory construct. As the Internet Safety Strategy acknowledges, the big boys are doing what government would expect them to be doing and ISPs have long since satisfied Government's requirements for site blocking. We have just been handed a new set of obligations under the Digital Economy Act for non-age verified pornography websites as well. What is an additional regulatory framework there to achieve? From the proposals that have come forward, I get the sense that it is to address inconsistencies and the long tail of smaller operators. You then need to think specifically about what incentives work for smaller operators and the balance as regards disincentivising them from entering the UK market. These are typically going to be San Francisco-based emerging companies that look at the UK market and think "take or leave". Let us get that balance right. More fundamentally, to return to my earlier point, let us not stop the debate at whether a new regulator has some requirement or powers to require information and set some transparency standards for content moderation. That is a partial response to our objective of creating a safer online environment. If we do not think more holistically about better equipping young people in that world, we will have failed them.

Lord Gordon of Strathblane: In the TalkTalk evidence, you say that only 14% of British voters think that social media is ultimately good for society. That is an alarmingly low figure. What would you recommend them to do to dramatically increase performance?

Iain Wood: I should stress it is not TalkTalk. That was a YouGov statistic that we quoted. I hesitate to lecture somebody else about their business model. One thing we have tried to do, as an ISP, is get ahead of the debate. Rather than be dragged grudgingly on to this territory and addressing the very genuine concerns of parents and children, we have tried to think it is completely understandable that people have these concerns, and we need to get ahead in terms of modifying the product and making sure we offer the product in a safe way.

If it is our TV product, you could have a walled garden where only children-appropriate content is available. If it is the internet, then we offer the filter—the wrap-around. We work through how we help parents apply that, as I talked about earlier. We then actively promote that to parents. We say, "You cannot become a customer unless you make these choices. Here is a whole host of information to help you understand it and here is some information you can have about broader risks that you might want to learn about regarding the online world". That does not solve every problem, but it does allow parents to see that we are taking this really seriously. We are imbedding safety by design into our core product rather than viewing it as an unnecessary evil.

I am sure if the big social media platforms were sat here today, they would say they are already doing that. I do not necessarily think that is being heard and understood by consumers. If you are passionate about technology and the benefit it brings to society, like we all are, you have to be equally passionate about understanding and mitigating the risks that undermine public confidence in that technology as well.

Adam Kinsley: I would point to the evidence that Doteveryone and Rachel Coldicutt gave to this Committee. There were some other statistics that I cannot remember off the top of my head. The public's trust is relatively low given what an amazing thing the internet is and what it does for us. Their conclusion is that there does need to be accountability. That is the only way that you can bring legitimacy back into the equation and put public confidence back into the system.

Q107 **Baroness Kidron:** My question is about design. When I asked about making the digital environment fit for childhood, you all went to safety. My question is about design. Can you stay away from safety and think about design. For example, in the written evidence from Sky it says, "The minimum standards should require that the strictest privacy settings should be 'on' by default, geolocation should be switched off until activated and privacy and geolocation settings must not change during either manual or automatic system upgrades". You have all talked about terms and conditions. What if your published conditions were on a statutory basis, so that if you continually fail your own published conditions, whatever they are, there would be some recourse? Forget about who regulates. If we reimagine design as being for societal reasons, a bigger picture, like Dan was talking about, is there something about the way that we are approaching this problem that is simply wrong? We are not looking at it from the ground up. I am afraid that is the first part of my question. Is anyone brave enough to answer?

Adam Kinsley: I can in a small way. You highlighted a detailed listed. I am not sure I quite like all of that long detailed list, because it is more of a state of mind. It is quite hard to do one-size-fits-all approaches as well. By way of an example, we built a kids app. I will say some of the things that I really like about it. When we developed it, we tested it every week or two. The developers went back and they got the young kids in to prod and push.

By using the same icons that are used on the modern internet, for example, the triangular play button, but making it very kid-friendly, we ended up with really good product. I cannot remember who I was talking to—it might have been you—with experience with BT and their engineers. When they got children and young people involved, it was a very different story. It is a lot easier for us to bring a new product to market with that philosophy in the front of our mind versus a large platform that was built quickly to get bought by another Silicon Valley giant, and before you know it, it is all a bit too late. That is the problem.

Iain Wood: That is why I have a slight concern about exempting SMEs from some of these debates, because that does two things. First, you risk creating such vanilla, big platforms that you force the problem somewhere else, which creates competitive distortions in the market. Secondly, and probably the more relevant point, is you say, "Fine, you do not have to worry about safety by design until you reach a certain scale". Then you are trying to retrofit. We all know retrofitting on to something is invariably more expensive, more difficult and ultimately probably less effective than embedding it from the outset. The end point has to be less around what have you managed to retrofit on to a product once you reach a certain scale and you find yourself on the front page of a newspaper, and how did you say to your product designers from the outset, "This has to be at the core of your mission"? If safety is not embedded in the product, it is not ready to launch.

Daniel Butler: The way you have framed the question is fascinating. We are starting to think about safety by design in our product development. Our kids' app is an example of that. There are different ways to characterise that too, such as accessibility by design and sustainability by design. This is clunky, but taking into consideration vulnerability in our design products. In relation to vulnerability, we have designed a Talk Protected line rental proposition that addresses the fact that older people primarily take only landline from us and are less engaged in the market, so we freeze their line rental for the lifetime of their being a customer with us. We add some vulnerability services if they have vulnerability challenges.

As a group of both pay TV platforms and ISPs, we are pretty mature in our suite of accessibility by design solutions, not least on the TV platform. That is a continually evolving challenge too. Why do we do that? Well, I would pinpoint a couple of conditions that that is a response to. One is an increasingly socially aware customer base that we are all trying to attract as customers. I do not have particular evidence to support that being the case, but I think there is a general feeling in corporates that there is a need to be more socially responsive. That has all kinds of positive externalities in terms of corporate behaviour. The second is some regulatory pressure. These topics are continually assessed by a regulator. Not all are subject to regulation or even ideas in the mind of the regulator. Sometimes regulators and politicians can shift corporate behaviour through self-pressure.

Adam Kinsley: Accessibility is a good example. Ofcom publishes a scorecard of how we do on our channels. It focuses minds.

Baroness Kidron: Funnily enough, that was the second part of my question. I was trying to get to the purpose of good design before we get to the regulation of it. Is there some value in thinking about things as universal standards or sets of criteria, or in rating privacy accessibility and vulnerability—whatever the schools of concern are—so that instead of terms and conditions that are hugely long and no one reads, you come to something and you think, "It is a green light, it is a red light", a bit like emissions and a bit like food? Is that a better soup for regulation—you know, pressure—to say, "We expect you to announce where you are in the system", for example?

Daniel Butler: What is great about that is that it maintains competitive dynamics in the development of those products. When you started with universal standards, I thought that removes any incentive on the operator, but where you ended up with a traffic-light system on the basis of which consumers could make competitive decisions about which operator fits with their values, not just their service requirements.

Baroness Kidron: But you need to have universal standards to understand what you are looking at. That was what I meant by that.

Iain Wood: I completely agree. When I talked about the ground rules before being a floor not a ceiling, the bare basics could be one out of five. That absolutely does not stop a provider aiming to be four or five out of five and using that for commercial advantage. When we launched our filters, and we were the first ISP to do it, we did it because we thought it was the right thing to do. But I would be lying if we said we did not also market it. We went out to parents and said, "If you are worried about inappropriate content on the internet, we have a product that can help you". There is no reason why something that is morally good cannot also be in the commercial interests of the organisation.

The Chairman: Mr Kinsley, do you have anything to add?

Adam Kinsley: No, I do not think so.

The Chairman: Sadly, I went slightly out of order. We have not made as much progress as I had hoped. Apologies to the Lord Bishop. Perhaps our witnesses can be reasonably concise in their answers, and if there are some elaborate issues, perhaps they could write to us. Lord Bishop.

Q108 **The Lord Bishop of Chelmsford:** I want to ask a question about the TV-like content, just to sharpen the focus on that for a few minutes. How should the video on demand services and the TV-like content be regulated? Should there be more of a level playing field in this regulation as compared with broadcast television?

Adam Kinsley: That is a good question; I think I should have that one.

The Lord Bishop of Chelmsford: It is one that probably affects you.

Adam Kinsley: Yes. TV-like and video on demand was a feature of the AVMSD Directive the first time around and has just been revised. The problem with it is that the definitions of "video on demand" and "TV-like" exclude some of the content we have been talking about today. Because of the narrow definitions of editorial control, Facebook is not in scope, for example. YouTube generally is not in scope either. While there was a model for broadcast which is heavily regulated and VoD a lot less so, it did not capture a whole swathe of online content, which is where people are viewing.

In the latest negotiations in Brussels for the revisions to the Audiovisual Media Services Directive, they included a new category of video-sharing platform. The problem with it is that it is so light touch, and there does not seem to be a mechanism for measuring any of the features of it, that it is a bit of problem. Historically, content protection has been where consumers expect it the most and where they are viewing the most, which has been the television screen. That is absolutely fine and right. As people are migrating and watching content online and on these platforms, it feels like the regulation has not caught up; that is, the detailed content regulation. Whether we ever get to implement the directive we have had in Brussels remains to be seen. It does not level the playing field at all, which is the nature of the slow-moving negotiations in Brussels.

The Chairman: Before others come in, what do you think should be done?

Adam Kinsley: The detailed content rules are not necessarily the problem we have to deal with here. I prefer to think about the much more holistic framework we have been talking about before, which looks at the concept of procedural accountability, which a number of witnesses to this Committee have referred to. It is a much better way of thinking of it than detailed rules every time, because you are always legislating for the last problem. That directive probably missed a trick, but the solution probably is not another detailed directive tomorrow.

Daniel Butler: My starting point on assessing what, if any, regulatory framework should apply to different types of VoD services is to think about the consumer expectation when they engage with those VoD services. We operate a VoD service which is heavily integrated as part of our pay TV proposition, as do the others. We integrate over the top applications like Netflix, Twitter and YouTube into our ecosystem. Our view is that customers have pretty sophisticated and different expectations when they engage with those different content platforms. When it comes to Netflix, Amazon Prime or our own VoD library, broadly speaking, the expectations that consumers have in terms of standards—and a reflection of the fact that some adult content should not be observable without some protections—are pretty equivalent in the linear world to the VoD world. Equally, we take steps to ensure prominence of public service broadcasting in our VoD library as well. The PSB apps have the most prominent content.

When you think about YouTube as a service or another user-generated content site, the user's expectation is different. The content that they are accessing is different. About 10% of the content that children watch on YouTube is what we would consider long-form content. The rest is music videos, funny videos and short-form content. Those are Ofcom statistics. There is a difference in user expectation, which necessitates a different regulatory solution. The final point I would make about VoD is the PSBs now have—and have had for while—propriety apps that increasingly compete with Netflix and pay TV platforms. There is a long-term policy question for Government and Ofcom about how you ensure universality of public service broadcasting content when they have an incentive to lock customers into their proprietary ecosystems.

Iain Wood: While those debates play out—and Adam alluded to the fact they are not going to move very quickly—there are things that we think we can do in the intervening period to better protect customers from inappropriate content. I referenced it earlier. One example would be our kids' TV service where, with the flick of a button, you go into a walled garden and the only content accessible in that is content that a parent has chosen to put in there. They can vary it. They can put in more educational programmes and take out cartoons. They can make sure that nothing that is adult content is accessible. There are ways that we can put a protective wrap-around layer around the child so the varying standards that exist do not necessarily have to harm the child.

Q109 **Lord Gordon of Strathblane:** How has age verification been implemented? Is it a good model for the future?

Daniel Butler: It has not been implemented yet, so it is hard to say whether it is a good or bad regulatory construct. We can say that it is a world first. It is a very new framework and model. All of us, as companies, have participated heavily in the development of that model and we want to see something emerge that is proportionate but effective. If we were to come back in six months' time, we would have a fuller view.

Adam Kinsley: I can give you one good and one bad. The good is that on the face of the legislation, age verification is left at a high level principle. It does not get into how it is done. That is a good model, setting out the idea that the website publishers will develop a model working with the regulator. That is not necessarily the right thing to prescribe on the face of the Bill. I think that is good. What I like less is that where there is noncompliance, the only named part of the value chain that is subject to any fines is the bit that is already regulated, which is the ISPs. That is symptomatic of this issue, that the regulatory framework is too narrow and does not extend beyond traditional players. Policymakers are always likely to come back to the bit that is already regulated.

Lord Gordon of Strathblane: Would it not be better to move away from age verification, as such, on to the equivalent of the BBFC system for films and have a series of walled gardens, leaving it up to parents to decide which walled garden their child is equipped to enter?

Iain Wood: In a way, that is what parental filters already provide. They provide a mechanism for parents to put a walled garden around any content that is accessed in the home. Success for age verification is not that you have a large block of websites that are blocked, because this will only ever apply to a minority of the internet. It will not block all porn. Success is that the major porn providers—it is a very concentrated market, with a handful of companies owning the most popular websites—change their policies and put age verification in place. We do not yet know whether they will do that or whether we will be using the backstop power to try to block them. If we come back in 12 or 18 months' time, I would like to think that the 100 most popular porn websites in the UK have age verification in place, not that the 100 previously most popular websites in the UK are now blocked and there are 100 more that have taken their place. Then it will have failed.

Q110 **Lord Allen of Kensington:** I would like to declare a historic interest. I served on the board of Virgin Media for a number of years. My question is around platform dominance and competition law. There has been a great deal of debate and discussion from a policy perspective in terms of the size and scale of these arguably dominant platforms. What are your concerns regarding what you flagged? What can we do about it? Maybe you could elaborate on some of your submissions. TalkTalk, you talked about the need for the CMA to review digital advertising. Sky, you talked about transparency, particularly around Ts and Cs and, in particular, business practices and ranking, et cetera. I would welcome Virgin's view in terms of areas of concern and practically what you think we can do about it. As you answer that, think about the fact that as we exit Europe, most of the competition legislations have been European-focused. What risks do we face there? How will we tackle that?

Iain Wood: I would start by saying their size reflects the fact they are offering very popular products. We should not be churlish and should congratulate them on that. They have been very successful. You know from your knowledge of the sector that TalkTalk has probably always been the strongest proponent of a competitive market. It will not surprise you to know that we think competition is also a good thing in other markets. In our view, it leads to better consumer outcomes. There probably are questions about whether the scale of the data advantage they have over new entrants, particularly digital advertising, is consistent with the principles of a competitive market. I know the consumer Green Paper is looking at these issues. It is probably right that we explore that. I am not prejudging the outcome, but it is the right debate to be having.

As I said earlier, I do not subscribe to the view that because they are global companies, we cannot regulate them. We compete against lots of global companies that have UK-specific regulation applied to them. Clearly, it will be easier and will probably lead to better regulation if there is regulatory consistency with Europe. The same would be true about aligning with the US. I do not think it is necessarily a Brexit question or a non-Brexit question. Irrespective of what happens with our future relationship with the

European Union, it will be in our interest to work closely with the European Union to try to ensure that the regulation that is almost inevitable is effective and gives consumers the protection they deserve.

Adam Kinsley: It seems us to that the framework in the UK works and is fit for purpose. We note that the Government are looking to give more of a strategic steer to the CMA to take bolder decisions. Some of the issues that have been raised by this Committee on online advertising may be looked at. Most of the Brussels interest is typically in the mergers and acquisitions, which is obviously a big part of this. In terms of the CMA's competence for competition behaviour, I had a look, and they are looking at 29 live non-merger cases at the moment. When you look at what they are doing with their consumer enforcement hat on, they are already looking at online hotel bookings, secondary ticketing websites and online gambling. I am not sure that it is necessarily a Brexit issue.

Lord Allen of Kensington: You raised some specific concerns. How would you look to address those? You talked about transparency, business practices, ranking, et cetera, et cetera.

Adam Kinsley: We are interested in the current work that the EU is doing on platform to businesses. I am not sure we necessarily have a significant stake in that. It is one of the things that we are following.

Daniel Butler: I cannot let Iain's assertion that TalkTalk is the primary advocate for competitive outcomes in telecommunications remain on the record. We built our own network, and that has been the single biggest driver of competitive outcomes in the UK market. There is a tendency to characterise big as bad in digital markets, which we do not subscribe to. Competition law orthodoxy does not just require dominance but the abuse of dominance. I would not necessarily comment on what the motivations of the European Commission are in a lot of the investigations. There has been commentary out there about some threadbare theories of harm that have emerged around some of the platforms.

Our starting point is to think about things from the consumer's standpoint and to think about how the consumer is served by digital markets as they have emerged. There is evidence of a substantial and underreported consumer surplus from the emergence of these digital platforms. In the main, consumers are getting higher quality products than they were prior to the emergence of the internet. In the main, those are free, compared with what they were paying prior to the emergence of the internet. That generates a substantial consumer surplus. Many of these services are substitutable, in terms of social media platforms, and yet consumers are willing to forgo significant value or income to retain those services.

I read a study last week that said that an average American citizen would forgo $50 of income per month to retain Facebook even though that is a substitutable service for another social media platform. That value increases where there is less substitutability, such as in Search, where it is substantially higher. The one Brexit-shaped question is that if you are in a market where you have very big content providers, in order to ensure that consumer outcomes are sustained and that there is good balance in the transmission of that content, you need to think about becoming a bit more comfortable with scale in the communications market. That might be consolidation of mobile with fixed or fewer operators in those two markets.

Baroness Kidron: I have noticed you have all talked about consumers. I am very aware that in Australia, consumer law and competition law sit together. Might part of the regulatory gap be better served by us looking at a similar system here?

Iain Wood: We have to be open to new models. The challenge with all this is that we are trying to apply physical world regulatory structures that imperfectly fit the new and emerging digital technologies. We have to be open to new ideas.

Daniel Butler: It feels very much like those two worlds have collided already, Baroness Kidron.

Baroness Quin: You feel that we will probably stay fairly close to Europe's regulatory system, but do you fear that we will lose influence in the shaping of that legislation in future? Or is it not a problem?

Iain Wood: After the last 24 hours, I think anybody trying to make predictions of what happens with the future relationship with Europe is destined to fail. I genuinely think it is too early to tell. We have much more experience of Ofcom, for instance. If you look at Ofcom's relationship with Europe, Ofcom has traditionally been probably the lead regulator in Europe. It has arguably been the most influential body in shaping telecoms regulation across Europe. That is a telecoms point rather than a platform regulation point, but it is clearly an example of where we previously had influence across pan-European regulation, which you have to assume will be less in a post-Brexit world.

Adam Kinsley: I want to quickly add to that. We would have less influence if we were not round the table and still taking the rules, but I see it as a big opportunity anyway. The DCMS has already set out the idea of a White Paper for online harms and is not waiting for the European Commission, which works in an entirely different way. It works with very prescriptive rules that go through the co-decision process, which is not really consistent with the much more proportionate evidence-based framework that we are talking about and, certainly, as in this report. I think it gives us the flexibility to create something that is far more pragmatic and fit for our market. I do not really see a concern. I think we can develop something that, once it is working and in practice, might be taken up by the Europeans.

The Chairman: I would like to move on. We promised our witnesses 90 minutes. Would you indulge us for a further 10 and two more questions? Then we will wrap the session up. You have given us very comprehensive and useful evidence.

Q111 **Baroness Chisholm of Owlpen:** I want to move on to neutrality. I have three short questions I want to ask you. How important is net neutrality? The EU Open Internet Regulation seeks to enforce it. Does it work? Is it sufficient? Post Brexit, ought we to have our own net neutrality law?

Iain Wood: It is very important. I hope there is consensus across the industry on that. Clearly, in all these debates we talked about earlier about protecting consumers, we are very conscious of the need to strike the right balance with net neutrality. We look at it very carefully. When we are looking at what tools we give to parents to block inappropriate content, we have to be very careful that we do not breach our obligations. Scams would be another example. Unfortunately, online scams are becoming a fact of life. We would like to be able to block certain platforms and tools that we know are predominantly used by scammers. We have tried to do that, but we have to be very cognisant of our net neutrality obligations.

In certain circumstances, we can default filter something but offer the customer the option to remove the filter if they so wish. In doing so, we can give them some advice about why we had applied it in the first place, which we hope protects them. That is an example of where it is quite tricky to strike the right balance. There is a tension between our obligations not to censor the internet—certainly not for commercial gain—with what we feel are moral obligations to try to protect customers. The regulations work in the UK as they stand. I do not think they need changing radically post Brexit.

Adam Kinsley: From my perspective, the debate about net neutrality was very live several years ago. In Europe, we followed the lead from the US. The European and particularly the UK market are very different. There is lots of competition at the retail end, which narrows the scope for abuse. In the UK, one ISP could not dominate and decide to be the gatekeeper because it would be punished. It is probably less of an issue in the UK than it was in the US. The European law might not be the best, but it sort of works. It does not feel like reforming it is the biggest priority right now.

Daniel Butler: I tend to agree with Adam. In principle, net neutrality is very, very important. In practice, it has not been a particular feature or consideration in the UK market. There is an economic argument about net neutrality as we look to the incentives for network operators to increase the capacity of their network in successive generations going forward. The question is whether consumers are willing to pay the premium in order for investors to receive a reasonable return on gigabit-capable networks or tens of gigabit-capable networks. Those are the kinds of networks that Government find superficially attractive and that would send us up the league tables. There is a version of the future in which, if consumers do not show a willingness to pay a premium for those higher-quality services, then the monetisation of those networks needs to come from somewhere, and the primary beneficiaries would be those distributing higher-quality content over those networks. The ability to recover from that end of the ecosystem would be necessary and potentially would have implications for the existing net neutrality framework.

Baroness Chisholm of Owlpen: Do you think we need to do anything here in the UK post Brexit? Do all three of you feel the same?

Daniel Butler: It is probably premature to start asking those questions.

Q112 **Baroness Bonham-Carter of Yarnbury:** Picking up on Adam's go-it-alone enthusiasm, I want to ask you all whether you think there are potential risks if the UK introduces regulation without the co-operation of international partners, particularly the European Union? How is this future divergence best managed? And then I have one other short question, but perhaps you can answer that first.

Adam Kinsley: It depends how it is done. The model which is described in some detail in this report is quite long—it is 35-odd pages. If it would be useful, on another occasion we could do a private briefing on the detail of it and get Mark back in to talk to you. But I think it can be done. Under recital 48, I think, the e-commerce directive already talks about duties of care for hosts to work with illegal content. We have not availed ourselves of that in the UK. Member states are allowed to do that. In article 16 it talks about codes of conduct being developed by member states; I think they are encouraged to do that, but we have not done it. It is wrong to think that member states are not allowed to act in this space. They are, but we have not done it, because the internet is just too difficult and different to regulate and that time has ended. There is now quite a strong consensus that we do need to do something. I think that we can act. The Germans have demonstrated that it can be done, but I am not sure that is the best way to do it. I understand they are going to be reporting on the efficacy of that next month, so we will see. Clearly, the more that you can do this at an international arena, the better, but that should not stop us from being bold ourselves.

Daniel Butler: I would just stress the importance of appropriate oversight in design. Baroness Kidron probed this earlier. The optimal framework is to have judicial oversight of the content that you are blocking. Some of the precedents that I have described are court order mandated, with a judge scrutinising the URL list. If we move beyond Germany just to the right and think about the political situation in Poland or Hungary, it is fair to be very nervous about precedents that we would be setting for content moderation on the internet, because some of the checks and balances in those nation states are being eroded by their Governments. Certainly if you went sub-judicial, you would have a very real prospect of those nation states engaging in censorship behaviour. Even at a judicial level, there is a question mark over judicial independence in those two nations.

Adam Kinsley: All of the global platforms are operating in those countries, and they are all taking decisions, as I described earlier, which you could argue are censorship, but they are doing it in a vacuum without any oversight. It is not the regulation that is offering the censorship. The censorship is already happening. I gave you the Wikipedia example where it was blacked out in Poland, I think. Should they be able to do that? Is Wikipedia a public utility that should be available? It is not the regulation that is offering the censorship. The regulation is offering the transparency and the oversight of the private companies that are taking decisions, maybe because of political pressure, but they are taking those decisions today. We are not requiring them to do that going forward, because they are already doing it.

Iain Wood: The important thing to stress is that in every stage of this policy debate there have been siren voices that said, "It is all too difficult. It will lead to censorship of the internet and the world as we know it will end". I remember sitting around tables five years ago when parental filters were being debated, and some of the internet service providers at the time accused us of censoring the internet, saying we were going to end the internet as we know it and we had no right to offer parents the option to filter porn in their homes. We did provide that, parents quite liked it, the world has continued turning and the debate has moved on. We cannot be afraid to tackle these things just because they are difficult. There is genuine public concern. It is appropriate for Parliament to say, "We have certain values, and we think they should exist online in the same way they do off it, and just because it is a difficult debate, we should not shy away from it".

Baroness Bonham-Carter of Yarnbury: Are there other international bodies that we should be looking to work with? We had evidence from Professor Wood that the UN's ITU, for instance, would prove to be a very difficult place for us to get agreement. You mentioned countries such as Poland and Hungary and how they are behaving. Are there other international organisations that you think we could usefully work with?

Adam Kinsley: There are a number of organisations that are worth talking to and sharing experiences with, but I am not sure that the right answer is to come up with an internationally agreed one, because we will be here in another 10 years waiting for that to happen.

Iain Wood: I think the answer almost is to get on and do it and find a model that works. I suspect we will find that other countries will then adopt that model.

Baroness Benjamin: Going back to age verification, I was surprised to hear that you had a few issues about whether it will work or not, because I was under the impression that most of the porn sites in the porn industry want you to have age verification to protect their business. Why do you feel it will be difficult for you to put it in place, and what are the barriers that will cause you not to be able to implement it?

Iain Wood: There are certain aspects of the regime that are still not decided, and that is a matter of concern for us. We would like to have those issues clarified very quickly so we know exactly what we are being asked to build. The actual block itself is quite straightforward for us to apply. I have very little concern that we can apply it, but there is a proportionality issue with the system whereby the BBFC simply will not have the resources to take enforcement action against every porn site on the internet, and therefore, initially, there will be a small list of companies that it is seeking to persuade. I do not want expectation to run ahead of reality in thinking that, on day one, every pornography website will be subject to enforcement action from the BBFC, because they will not. It will be the list of the most prominent and popular websites. It will be a tool and we will find out how effective it is. Hopefully, the major providers and platforms will change their business models and be a success, but we have to be cautious in thinking that it will be a catch-all that solves every website on the internet.

The Chairman: I thank our witnesses for the evidence that they have given us today. It has been a very interesting session and we have raised lots of issues. I also thank you for the courtesy you have shown in referring to our previous reports and the evidence we have received, and for the obvious preparation with which you have come here to answer our questions. The evidence has been very useful and we welcome it very much.

Daphne Keller, Stanford Law School Center for Internet and Society - written evidence (IRN0052)

Question 1: Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

1. Internet-specific regulations, or Internet-specific rules within broader regulations, are eminently possible and in many cases desirable. It is essential, however, that such laws be shaped in response to clearly defined and understood harms. Too often, calls for "platform regulation" conflate distinct problems, many of them already addressed in existing bodies of law such as competition, privacy, defamation, or electoral regulation. If these time-tested legal doctrines fail to address evolving Internet-based threats, lawmakers can and should adapt them to changed circumstances – as was done in the U.K. Defamation Act of 2013. But they should be wary of proposals to scrap precedent and lessons of the past in favor of new rules, drafted from scratch to address hazily defined threats.

2. This submission addresses precedent and lessons from the law of Intermediary Liability, which establishes Internet platforms' legal responsibility for content shared online by their users. I am familiar with these laws in part through my previous work as Associate General Counsel to Google. In that role, I counseled the company on Intermediary Liability laws ranging from the E.U.'s eCommerce Directive to the U.S. Digital Millennium Copyright Act to India's Information Technology Act. I also testified about Google's content removal practices to the U.K. Parliament's Joint Committee on Privacy and Injunctions and to the Leveson Inquiry. In my current position as Intermediary Liability Director at the Stanford Center for Internet and Society (CIS), I continue to research and write about these laws.[1110] My team at Stanford maintains the World Intermediary Liability Map, the primary online resource tracking global legal developments in the field.[1111]

3. Because Intermediary Liability law for the Internet has existed for only a few scant decades, it is unfamiliar to many practitioners. Nonetheless, experience with laws around the world during that time – as well as earlier experience with "analog intermediaries" such as bookstores or telegraph operators – can provide important lessons.[1112] This submission will focus on what guidance Intermediary Liability precedent might provide as lawmakers consider future regulation.

[1110] CIS is a public interest technology law and policy program at Stanford Law School. A list of CIS donors and funding policies is available at https://cyberlaw.stanford.edu/about-us.

[1111] http://wilmap.law.stanford.edu/

[1112] A U.S. example is *Smith v. California*, 361 U.S. 147, 153 (1959) (rejecting strict liability for bookstores in obscenity case).

Question 2: What should the legal liability of online platforms be for the content that they host?

4. Lawmakers enacting Intermediary Liability laws generally seek to balance three high level objectives. The specific liability rules for any country will depend on its legislators' choices among those objectives, and on its judiciary's interpretation of fundamental and human rights laws.[1113]

Objectives

5. The first and most obvious objective of Intermediary Liability law is to reduce the spread of harmful and illegal material online. This goal is broadly served by expanding intermediaries' liability -- though poorly-crafted liability rules can instead, perversely, prevent platforms from moderating content.[1114] The second objective is to support innovation and competition. Legal regimes that expose platforms to substantial liability for user content deter investment in innovative technologies.[1115] They can also reinforce the advantages held by incumbent platforms, and make it harder for smaller competitors to gain a foothold.[1116]

6. The third and most legally complex objective to be balanced in Intermediary Liability law is the protection of Internet users' rights to free expression and information. Internet "notice and takedown" systems operated by platforms are notoriously subject to abuse by those seeking to silence critics, opponents, or competitors. The government of Ecuador, for example, has used spurious copyright notices to suppress criticism and videos of police brutality.[1117] Empirical studies suggest that platforms far too readily honor such requests – which is not surprising, given the low cost of compliance and the high cost of legal assessment and exposure.[1118] This dynamic, and the concern that private platform "adjudicators" will systematically throttle lawful information, has led courts around the world to conclude that imbalanced Intermediary Liability laws conflict with states' human rights obligations. In particular, several courts and legislatures have rejected strict liability models that would require platforms to actively monitor users' online

[1113] A detailed discussion of U.K. human rights law constraints on state and private actors in Internet content removal can be found in the Internet Watch Foundation's 2014 human rights audit, by former Director of Public Prosecutions Lord Ken Macdonald. https://www.iwf.org.uk/what-we-do/who-we-are/human-rights-audit.

[1114] Paul Ehrlich, *Communications Decency Act Section 230*, 17 Berkeley Tech. L.J. 401 at 404 (1990s case law in U.S. created "paradoxical no-win situation: the more an ISP tried to keep obscene or harmful material away from its users, the more it would be liable for that material.")

[1115] https://www.strategyand.pwc.com/media/uploads/Strategyand-Impact-US-Internet-Copyright-Regulations-Early-Stage-Investment.pdf.

[1116] Engine, *Startup Advocates Address Implications of Sex Trafficking Legislation on Tech* (Feb. 26, 2018), http://static1.squarespace.com/static/571681753c44d835a440c8b5/t/5a9608df419202d2af99166f/1519782111557/FOSTA_SESTA+Media+Advisory.pdf.

[1117] https://www.hrw.org/news/2014/12/15/censorship-ecuador-has-made-it-internet.

[1118] http://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws.

communications.[1119]

Legal Models

7. National laws defining Intermediary Liability often share a basic architecture. They typically immunize platforms only if they maintain a sufficiently arms-length relationship with user content. Under most (but not all) legal models, platforms become liable if they fail to take action once they know of illegal content's existence.

8. Where national laws often diverge is in their conceptions of platforms' *knowledge* and their prescriptions for platforms' *procedures* upon learning about potentially illegal content. These elements of Intermediary Liability law provide the "dials and knobs" for judges and lawmakers to fine-tune legal requirements and balance the three considerations discussed above: harm prevention, innovation, and free expression rights.[1120]

9. Courts, including European courts, sometimes assume that any allegation of wrongdoing gives a platform knowledge sufficient to strip it of legal immunities. This is too lax a standard under applicable CJEU precedent, which finds no knowledge when a notice is "insufficiently precise or inadequately substantiated."[1121] Putative sources of knowledge can also fail the mark under other bodies of law, such as defamation. As one U.K. court noted, a platform is hard pressed to determine the truth when "faced with conflicting claims … between which it [is] in no position to adjudicate."[1122]

[1119] *See, e.g.*, *Rodriguez M. Belen c. Google*, (2014) R.522.XLIX, (Argentine S. Ct. rejecting requirement for platforms to proactively monitor user speech on grounds of information rights); *Shreya Singhal v. Union of India*, (2015) 12 SCC 73, at ¶117 (Indian S. Ct. construing statute on free expression grounds to mandate removal only based on government order); Marco Civil da Internet, Brazil, Federal Law no. 12.965; Law No. 20.435, Chile, amending Intellectual Property Law.

[1120] A third possible variable in national law comes from definitions of which services are eligible for immunity, based on technical specification or on "neutrality" or "passivity". As many commentators including myself have observed, these standards are extremely difficult to apply in meaningful ways to Internet hosts. *See* https://knightcolumbia.org/content/toward-clearer-conversation-about-platform-liability Section II.A. The leading CJEU case for the E.U.'s "passivity" standard under the eCommerce Directive found that Google's provision of ads, which the company organizes and ranks as a paid service, was sufficiently passive and thus immunized. *Google France v. Louis Vuitton*, C-236/08C-238/08 (2010).

[1121] *L'Oréal v. eBay* at ¶ 122.

[1122] *Davison v. Habeeb* ([2011] EWHC 3031 (QB) para. 68; see also *Bunt v. Tilley* ([2006] EWHC 407 (QB)) (Mr. J. Eady) para 72 ("in order to be able to characterise something as 'unlawful' a person would need to know something of the strength or weakness of available defences"), quoted in *Kaschke v. Gray* ([2010] EWHC 690 (QB)) ; *compare Tamiz v. Google Inc.* ([2013] EWCA Civ 68) (blogging platform can be liable in defamation without consideration of eCommerce hosting defenses or knowledge standard).

10. Some courts or lawmakers around the world have drawn brighter lines, saying that certain legal claims should never be *de facto* adjudicated by private companies. Under these legal frameworks, a platform is not said to "know" that content is illegal until a court has assessed the claims and defenses. Chile applies this rule to copyright, for example, and Brazil applies it for most claims other than copyright and non-consensual pornography.[1123]

11. Variations in removal *processes* – what a platform does when it becomes aware of potentially illegal material – are equally important. Some national laws offer no guidance for this situation. Others prescribe very specific steps, which can include notice to the accused speaker and an opportunity to "counternotice" or challenge wrongful removals. The U.S. DMCA offers perhaps the most detailed legal model of this sort.[1124] Human rights officials and civil society groups around the world have embraced procedural rules as an essential mechanism for laws to adequately protect free expression rights.[1125] The widely endorsed Manila Principles, developed by civil society groups around the world, offer a menu of procedural options to protect Internet users' rights in private notice and takedown systems.[1126]

12. Counternotice mechanisms alone do not adequately protect against widespread erasure of lawful material. The publicly available data suggests that counternotice is rarely used, and thus fails to remedy most erroneous removal of lawful speech.[1127] It is particularly unlikely to be effective in situations where the information rights of listeners, rather than the expression rights of speakers, are primarily at stake. When a witness to human rights abuses in Myanmar posts a video documenting what she has seen, for example, she may have limited ability or willingness to take part in a formal counternotice process.

13. More effective protection comes from public transparency, which permits diffuse stakeholders to crowdsource the job of error correction. For this to work, though, platforms must disclose clear and specific information about what content has been taken down. The Lumen Database at Harvard Law School provides the world's leading archive of such information, and has been the foundation for some of the most important scholarship tracking platform behavior in notice and takedown systems.[1128] As platforms increasingly expand their removal policies and

[1123] See *supra* note 9.

[1124] 17 USC 512.

[1125] *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN (2016), *available at* https://perma.cc/44AY-ZX9G (Manila Principles "establish baseline protection for intermediaries in accordance with freedom of expression standards"); *Standards for a Free, Open and Inclusive Internet* (2017), OAS Office of the Special Rapporteur for Freedom of Expression.

[1126] www.manilaprinciples.org.

[1127] http://cyberlaw.stanford.edu/blog/2017/10/counter-notice-does-not-fix-over-removal-online-speech.

[1128] www.lumendatabase.org; Brief of *amicus* in Perfect 10, Inc. v. Google Inc. listing scholarly work as of 2010, https://www.eff.org/files/filenode/Perfect10_v_Google/2010-12-21p10vgoogle_amicus.pdf. By far the most comprehensive empirical research on notice and takedown is Jennifer Urban et al's 2016 *Notice and Takedown in Everyday Practice*.

operations, NGOs have called on them to commit to more effective transparency measures.[1129]

14. The optimal combination of knowledge standards and procedural protections under Intermediary Liability law may vary depending on the kind of unlawful content at issue. For highly dangerous and easily recognizable material, it is more reasonable to expect platforms to act unilaterally. All countries I am aware of require platforms to swiftly remove child sexual abuse images, for example. More exacting standards are appropriate, on the other hand, when platforms remove citizen speech on matters of public concern.

15. Beyond these high level considerations, I note particular observations on several matters under current discussion in the U.K.

16. **Terrorism:** Online materials that can promote or facilitate violent terrorist attacks pose one of the most serious concerns for platforms and governments today. I address this issue in detail in a recent submission to the European Commission, which is included as an appendix to this submission [appendix not attached].[1130] As discussed there, over-removal poses particular threats in this context. Errors can silence important political speech – like videos posted by Syrian human rights workers to document war crimes and enable future prosecutions.[1131] Over-removal also has foreseeable disparate and discriminatory impact on Internet users based on their ethnicity, language, or religion. In addition to fundamental rights concerns, this raises pressing and unanswered questions about the ultimate security benefits of aggressive online content elimination. Overzealous content removal efforts carried out in the name of public safety and security may in fact undermine our safety.

17. **Filters:** As also addressed in the Commission filing, reliance on technical filters, machine learning, or other automated tools exacerbates many of the problems with notice and takedown. Filters are blind to context, and cannot distinguish news and educational uses from illegal or rights-infringing ones.[1132] While human review provides some degree of correction for inevitable filtering errors, we already know of substantial problems with bias and over-removal in

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628. This qualitative and quantitative study addresses U.S. copyright removals, which make up by far the largest available data set, but many of the trends it identifies are generalizable to other legal claims.

[1129] https://www.theverge.com/2018/5/7/17328764/santa-clara-principles-platform-moderation-ban-google-facebook-twitter.

[1130] http://cyberlaw.stanford.edu/files/publication/files/Commission-Filing-Stanford-CIS-26-3_0.pdf. [Appendix not attached]

[1131] Malachy Browne, "YouTube Removes Videos Showing Atrocities in Syria," The New York Times, 22 August 2017; Scott Edwards, "When YouTube Removes Violent Videos, It Impedes Justice," *Wired*, 07 October 2017.

[1132] http://www.engine.is/events/category/the-limits-of-filtering-a-look-at-the-functionality-shortcomings-of-content-detection-tools (discussing failures of audio and video filters); https://cdt.org/files/2017/11/2017-11-13-Mixed-Messages-Paper.pdf (discussing failures of text filters).

human-operated systems. Moreover, it may be naïve to expect companies to continue to spend heavily on high quality human review efforts, or indeed on human review of any sort.

18. **Media Regulation:** Existing media regulatory models could provide valuable precedent, language, or structure for laws governing Internet platforms. In some respects, however, traditional media and online platforms differ fundamentally and cannot be governed by the same laws without eliminating some of their most important functions. The most important differences relate to the expression and information rights of ordinary Internet users. The individuals who are able to share their political opinions, creative output, or cat videos on today's Internet platforms typically have no voice at all in traditional media. This is because of the vast difference in scale between the two kinds of operations. That same difference in scale makes possible the responsibility that broadcasters, newspapers, and other media actors have traditionally assumed for editing and curating content.

19. The functional differences between traditional media and Internet intermediaries are in some ways eroding. Mega-platforms like Facebook or YouTube sometimes create or commission their own content, or use algorithms to sequence content or make recommendations. Newspapers act as platforms when they open up comment forums to users on their websites. This convergence may mean that aspects of traditional media regulation become relevant or useful for governance of Internet platforms. But for the specific function of processing user-generated content, the liability rules designed for traditional media are profoundly ill-suited. Applying them could render platform operations impossible. It could also run afoul of the European Convention on Human Rights.[1133]

Question 8: What is the impact of the dominance of a small number of online platforms in certain online markets?

20. For Intermediary Liability purposes, consolidation of online platforms makes content removal errors and suppression of lawful information far more consequential. Internet users wishing to seek and impart information online have fewer viable avenues for doing so today than they would have had a decade ago. If their accounts or posts are banned from those channels, they may struggle to make themselves heard.

21. The large, multinational corporations that control important channels of online communication are also in some ways uniquely vulnerable to interference that

[1133] *MTE v. Hungary* (2016) E.Ct.H.R. 82, http://www.bailii.org/eu/cases/ECHR/2016/135.html (strict liability or monitoring may not be mandated in case of defamatory speech in news forum comments); *compare Delfi AS v. Estonia* (2015) E.Ct.H.R., http://www.bailii.org/eu/cases/ECHR/2015/586.html (strict liability permissible in case of unprotected hate speech in news forum comments).

harms the rights of Internet users.[1134] The biggest platforms have offices and assets around the world, in countries with widely divergent conceptions of human rights. This gives governments in places like Vietnam, China, Russia, and Turkey a degree of leverage they would never have had in a more decentralized Internet. In 2016, for example, Malaysia blocked the blogging platform Medium because it refused to take down allegations of political corruption published by a London-based investigative journalist.[1135] Medium effectively sacrificed revenues from the Malaysian market in order to protect the publisher's rights. A dissident whose home country had more substantial economic power over a hosting platform might not be so fortunate. Internet consolidation reduces the number of chokepoints that can be targeted by anyone from state actors to criminal hackers to disrupt the flow of online information.

11 May 2018

[1134] While public discussion of hosting consolidation tends to focus on edge providers like Facebook or YouTube, consolidation of technical hosting services such as Amazon Web Services creates similar vulnerabilities to state pressure or technical failure, affecting a the wide array of sites. *See, e.g.*, https://www.recode.net/2017/3/2/14792636/amazon-aws-internet-outage-cause-human-error-incorrect-command.

[1135] https://www.engadget.com/2016/01/28/malaysia-medium-block-explainer/.

Subforum LLC – written evidence (IRN0013)

PLATFORMS HARVEST TOO MUCH ATTENTION

Q1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

- Attention Capitalists are corporations who harvest **human attention** as a resource and then sell it on the internet. Attention is easily exploited by using **variable rewards** to ensnare a person's focused attention as long as possible, and by taking advantage of natural human **vigilance** to compel users to come back as frequently as possible. Harvested attention is capitalized through the display of targeted ads. The attention economy has grown unchecked; its economics have created or complicated a host of societal issues, because corporate and societal goals aren't aligned:

Societal Goals	**Online Platform Goals**
Inform each person about a wide array of issues and viewpoints	Capture and hold each person's interest as long as possible
Uphold individual privacy rights	Sell users' private interests and data
Balance online time with family and community time	Infiltrate family and community time

- Dominant attention capitalists have built useful & powerful platforms that enable people to connect and share ideas. They've had a transformative impact on how people relate and communicate. Large platforms—Facebook, Twitter, YouTube, et.al.—achieved scale by aggressively harvesting user attention. Such harvesting is exploitative in a sense, because platforms can take as much attention as they can get without considering the long-term health of the user or the society.

- It is in a platform's long term interest to regulate attention consumption because it would generally create healthier users. And yet, platforms are not self-regulating because to do so would conflict with their short-term financial interests and advantageous economic positions. Government must compel more sustainable practices in the attention economy, in several areas:

  - **Privacy:** how and where platforms can share user data and metadata, building upon the implementation of the EU's General Data Protection Regulation.
  - **Moderation:** What content can be displayed, when, and to whom.
  - **Consumption:** How much human attention can be harvested by a platform.

- This evidence will focus on **(3.2.)** and **(3.3.).** Regulation of these areas would improve the quality and safety of content and encourage healthier behaviors by platform users. Regulations should focus on standards for measuring, evaluating, sustaining and reporting upon the **health** of publics that use online platforms, and the use of health measures by platforms to guide individual user behavior.

Q3A. How effective, fair and transparent are online platforms in moderating content that they host?

- **EFFECTIVENESS**: The current best practice is to employ a sizable team of human moderators who can review flagged content and decide whether to display that content. Flags are generated by the curation team itself, reports from the user community, and by automated detection systems. This type of moderation is difficult to scale because of the massive volume of data. Artificial Intelligence (AI) systems that leverage Natural Language Processing, Entity Resolution, Visual Analysis, etc, to improve effectiveness and scalability are being actively developed, but are not yet effective on their own. A reasonable system should perform at high percentage of Precision/Recall (P/R)[1136] in finding malicious content. Facebook, Twitter, Google, et. al. don't share P/R results; perhaps they should. Open moderation by the user community—e.g. "83% of our users believe this content is malicious"—is an alternative, scalable approach but introduces privacy issues and will tend to have the opposite of the desired effect, because users embrace ideas that come from cultural or political groups they identify with, more than they would embrace truth itself.[1137] [1138]

- **FAIRNESS**: Current moderation systems favor freedom of expression. They have open content guidelines[1139] and only remove violative content. Platforms are fair to **content creators** in this way. They are unfair to **content consumers***.* Consumers are not enabled to see or edit the *metadata* which the systems generate and then attach to their profile in order to target content to them. They also can't see how that metadata is shared with advertisers. Consumers only see a subset of content that has been targeted to them, because content accumulates so quickly that it is impossible to view it all. Online platforms have thus become the de facto gatekeepers for when and where content is seen, if at all. In practical terms, targeted filtering systems provide a form of content moderation, by enabling content promotion and suppression in ways that platforms like Facebook actively implement.[1140] Platforms are incentivized to prioritize and present content that compels engagement and increases advertising revenues. The

[1136] P/R is a standard measure of AI effectiveness - https://en.wikipedia.org/wiki/Precision_and_recall

[1137] Identity Science and why humans are attracted to fake content - https://psyarxiv.com/ak642/

[1138] https://www.techdirt.com/articles/20180131/22182339132/implementing-transparency-about-content-moderation.shtml

[1139] Facebook's Content Guidelines - https://www.facebook.com/communitystandards/introduction/

[1140] Ranking sources by trust - https://www.buzzfeed.com/bensmith/facebook-has-begun-to-rank-news-organizations-by-trust most engaging content tends to be cultural identity affirmative material.[1141] This material creates echo chambers that render a biased reality and conform to the user's system of beliefs. Echo chambers are resilient but not illuminating, and while affirming, they actually violate user expectations that the platform experience reflect societal diversity.

- **TRANSPARENCY**: Platforms are opaque in their implementation of moderation because transparent systems are easier to manipulate. Platforms could give users more insight into the nature of content by displaying more metadata that describes the content—e.g., topics or source credibility. AI systems will soon be able to understand the **polarity** of a particular story or event by contrasting the sentiment of different publications, authors, and statements about or within a piece of content. Polarity is particularly powerful because it doesn't align to one political or cultural group versus another—say, liberals vs conservatives—it would simply illuminate for all users how much the views of various groups diverge on a particular topic or piece of content. This can compel users to reflect upon identity and beliefs.

Q3B. What processes should be implemented for individuals who wish to reverse decisions to moderate content?

- A user-driven **arbitration process for polarized content** where representatives of the polarized cultural/political/social groups discuss moderation decisions to be made or reversed. If the group is unable to make a consensus determination, the decision gets raised to a new set of representatives. Once a decision is made, consensus metadata—arbitrator notes, content veracity, topic tags—could be displayed along with the content. Removed content could be replaced by a placeholder page, but with the metadata still made available to users.

Q3C. Who should be responsible for overseeing this?

- Arbitrators would ideally be a subset of the community of platform users who have opted to have their individual and cultural identity publicly verified.

- A small team of moderators employed by platforms would oversee arbitration.

Q5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

[1141] Quantitative evidence of echo chambers on Facebook - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2795110

MEASURE 1: ENCOURAGE USERS TO CLOSE THINGS

- The most powerful measure that online platforms can take to improve the overall health of society is to compel occasional disuse of the platform itself. People who spend too much attention on platforms are more distracted, stressed, depressed, even desocialized.[1142] Platforms can cultivate more balanced usage behaviors and better overall health by encouraging users to reorient their attention back into the physical world. In an ideal world, platforms are just one part of a diverse blend of online/offline life experiences.

- All major online platforms use **variable rewards** to harvest user attention.[1143,1144] To understand variable rewards, imagine a slot machine. You put in a coin. You pull the lever. Do the three shapes all match? Nope? OK, pull again. How about this time? That's the hook: the anticipation of getting a reward (whether or not we actually get one) increases the dopamine levels in our brains, which compels us to keep doing the thing that got us a reward before. We humans are particularly responsive (higher levels of dopamine) to unpredictable rewa;rds that are offered on a variable, non-fixed schedule.[1145] [1146] Some examples of variable rewards in online platforms are:

Behaviors the Platform wants to Reinforce	**Variable Reward Offered**
Scrolling Facebook's news feed / pull to refresh on Twitter, etc.	An interesting or amusing update
Posting, commenting, or responding	Gratifying likes and other responses
Checking messages or notifications	Receipt of inbound communication

- Platforms can use variable rewards to give back user attention just as much as they've used them to capture attention. By inverting the 'payment model' of variable rewards—creating **Inverse Variable Rewards**[1147]—platforms can reinforce healthy behavior change. Instead of asking users to pay with attention, platforms can ask them to pay with abstinence from use. Instead of being rewarded for looking at, tapping on, or posting something, users

[1142] For example - https://hbr.org/2017/04/a-new-more-rigorous-study-confirms-the-more-you-use-facebook-the-worse-you-feel

[1143] Use of variable rewards online - https://www.nirandfar.com/2012/03/want-to-hook-your-users-drive-them-crazy.html

[1144] Variable Rewards and Behavior Change - https://www.1843magazine.com/features/the-scientists-who-make-apps-addictive

[1145] See B. F. Skinner's Operant Conditioning Chamber - https://en.wikipedia.org/wiki/Operant_conditioning_chamber

[1146] https://news.vanderbilt.edu/2004/05/07/its-a-gamble-dopamine-levels-tied-to-uncertainty-of-rewards-59664/

[1147] Inverse Variable Rewards - https://hackernoon.com/inverse-variable-rewards-1e6a101790bf could be rewarded for not doing those things. When individual usage patterns begin to be unhealthy, we can leverage addictive design patterns to incentivize disengagement, balancing usage habits over time simply by nudging users to unplug. This inversion of variable rewards can compel healthier, more balanced usage and help users develop more trust in a platform.

- Example #1: Imagine that the Facebook newsfeed had a bottom, discoverable after some reasonable amount of scrolling or swiping, with a note saying when to expect more content. Facebook could implement an inverse variable reward into this pattern: the possibility of getting a reward when the new content gets loaded. The longer the user waits for more content, the more likely the reward.

- Example #2: Curb trolling or abuse by preventing offenders from seeing new content until they refrained from the abusive behavior for a meaningful period of time.

MEASURE 2: RECOGNIZE AND SUPPORT VIGILANCE

- All types of heavy online platform usage are described as addiction. Platforms do have built-in addictiveness as detailed above. But users are not just addicted: they are also (and more often) being vigilant.

- Vigilance is the allocation of significant attentional resources to perform sustained watchfulness. This watchfulness is extreme and associated with self-preservation; for example, a zebra keeping eyes and ears open for predators while also grazing. For humans online, it is not the physically embodied self that we seek to preserve by vigilantly monitoring online platforms. Rather, it is the digitally social self, comprising the increasingly numerous facets of our own sense of self (and self-worth) that are established and maintained through online platforms.

- Socialization amongst humans involves a number of mechanisms, like Identity Performance—an iterative process wherein we do something, observe how people respond, and then adapt accordingly.[1148] Identity performance provides fluid and instantaneous social feedback that helps us cultivate our understanding of how we should act but also who we are—this happens online just as readily as it happens in the physical world.[1149] Unlike in the real world, though, inbound communications and social responses online are not instantaneous and can come at any time. Responses are easy to miss: people must commit sustained partial attention to monitor for cues that someone may have said something important to them, or offered a crucial response to a post or a message.

[1148] Description of Identity Performance - https://en.wikipedia.org/wiki/Identity_Performance

[1149] Discussion of online socialization - https://www.danah.org/papers/WhyYouthHeart.pdf

- Thus users become vigilant, feeling extremely watchful over platforms and mobile devices, checking for notifications even when they didn't hear or see one, every day.[1150] Addictive design patterns may keep you on your device for longer than you'd planned, but vigilance is what causes you to look at your device in the first place.

- Vigilance is uniquely exhausting for users[1151]: it creates sustained cognitive load on attention. There are specific design guidelines that platforms can follow to support vigilance more responsibly.[1152] For example: a user may naturally lose interest in the things a platform is sending notifications about. If the user stops taking the action the platform is asking them to take in a notification, then the platform should proactively turn off the notifications and tell the user why they did it. Rather than sending notifications immediately, platforms should ask the user when is a good time to send notifications, then batch up notifications and send them when it's convenient. Platforms should make it easy for users to suppress notifications.

MEASURE 3: ADOPT BETTER HEALTH METRICS.

- All technology organizations use metrics from product instrumentation to understand how their products are being used.

- Online platforms focus on **business growth metrics** that represent the scale and reach of their business, which equates to success. Success is measured by frequency of use, recency of use, and volume of activity. These metrics have near-term criticality for platforms because they can be correlated to advertising revenues and pricing.

- Online Platforms should also define, track and publish **societal health metrics** that show the long-term impacts of usage. Twitter has begun exploring this.[1153] Health metrics must highlight things like reasonable levels of individual usage, levels of activity for different political or extremist groups, amount of hateful content, and P/R numbers for content detection. Reported health metrics would make platforms accountable for long-term health and user benefits. Focusing on health benefits helps ensure that platforms are delivering value to the user, and not simply exploiting their attention. As such, health metrics would be a promising focus for regulation.

Q7. In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

[1150] Discussion of vigilance and smartphones - https://hackernoon.com/blind-to-vigilance-7e9b72ab2ad4

[1151] User impacts of vigilance - https://www.ncbi.nlm.nih.gov/pubmed/18689050

[1152] Qualitative evidence - http://interactions.acm.org/archive/view/november-december-2014/are-mobile-users-more-vigilant

[1153] Twitter's Health Metrics RFP - https://blog.twitter.com/official/en_us/topics/company/2018/twitter-health-metrics-proposal-submission.html

- Publish societal health stats as discussed above, on at least a quarterly basis.

- Allow users to see all generated metadata that is attached to their profile and used for targeting advertisements and content. Describe to users the logical and algorithmic rules for how & when content is selected by the platform on their behalf.

- Give users visibility into how much content they're missing via filtration. Platforms should persistently show the overall size of the accessible content corpus in context.

- Enable and encourage users to assert the things that are most important to them. Content preferences should be managed as an ongoing conversation between the platform and the user, not through a settings page that has been buried somewhere. Preferences should not be treated as a set-it-and-forget-it feature. It's better to wait until a user shows interest in specific features or content, and then ask if they'd like to receive alerts or more information about those things.

Acknowledgements

My colleagues Sherry Turkle, Bryant Wolf, Julie Sargent, Jenni Won provided valuable feedback and helped me refine this evidence.

4 May 2018

Professor Richard Tait – written evidence (IRN0042)

1. This submission focuses on the issues of specific regulation for the internet (Question1) and the effect of the UK leaving the EU (Question 9). The two are closely linked as the UK as a member of the EU is at present actively involved in Europe-wide efforts to deal with all the issues raised by the Committee, with Sir Julian King, EU commissioner for security, playing a leading role.

2. The Committee is right to raise the question of 'platform or publisher?' It is central to the argument how far content, particularly news content, on the internet can and should be regulated. There is no doubt that for the last two decades the conventional wisdom has been that online platforms do not exercise editorial control and should not be regarded as publishers. The law in the EU and elsewhere has shielded them from the legal obligations of print and broadcast publishers.

3. In reality, the internet businesses, which now dominate much of the media world, have always been both platforms and publishers. Over the years their publishing role has overtaken their platform role in terms both of revenue and of political and social impact. The Committee's recent report into the advertising market shows clearly how Facebook and other digital media companies are replacing traditional broadcasting and print media in the UK; in the US 45 million adults now take some of their news from Facebook. The recent scandals over fake news, interference in elections and improper use of data mean the argument that these are purely technology companies to be regulated only as tech businesses is no longer sustainable.

4. On 10 October last year Dame Patricia Hodgson, the then chair of Ofcom, told the Commons digital, culture, media and sport committee that her personal view was that internet businesses such as Google and Facebook were publishers. She revealed that the Board of Ofcom had discussed internet regulation at its most recent strategy day, though any decision on this was a matter for government.

5. In his evidence to the US Congress on 10 April, Mark Zuckerberg, Facebook's Chairman and CEO, accepted, for the first time, that Facebook was responsible for its content. Although he pointed out that Facebook did not make the content and said he still saw Facebook as a tech company not a media company, he accepted it had a responsibility to its users. "It's not enough just to build tools. We need to make sure that they're used for good'. He also accepted the need for regulation 'I think the real question, as the Internet becomes more important in people's lives, is what is the right regulation, not whether there should be or not'.

6. The EU takes the same view – the European Commission on 24 April said that 'some platforms have taken on functions traditionally associated with media outlets, entering the news business as content aggregators and distributors without necessarily taking on the editorial frameworks and capabilities of such outlets'. The 'platform or publisher?' debate has been settled once and for all – the internet businesses, which dominate the global media scene, are, effectively, publishers and should be treated as such. The argument now is not about whether some aspects of the internet should be regulated, but how.

7. In the current climate, the internet businesses are under intense international pressure to show they can regulate themselves effectively. In the area of data regulation, Mark Zuckerberg has already committed Facebook to applying the EU data standard - GDPR - across Europe and to make the same controls available worldwide. It is at least possible that the EU could take a similar global lead in the area of disinformation (fake news and political manipulation) given that the EU experience of content regulation may be more relevant in this context than what happens in the US, where broadcast news regulation has virtually disappeared.

8. The European Commission's initial proposals, **Tackling online disinformation: a European Approach,** published in April 2018, envisage a comprehensive programme of action. Measures include greater emphasis on fact checking, support for high quality journalism, and better media literacy. But the most important new requirement is that the internet businesses reform themselves. It says 'The Commission calls upon platforms to decisively step up their efforts to tackle online disinformation. It considers that self-regulation can contribute to these efforts, provided it is effectively implemented and monitored' There will be a EU-wide Code of Practice on Disinformation by July this year with a view to producing measurable effects by October 2018. The Commission adds that 'should the results prove unsatisfactory, the Commission may propose further actions, including actions of a regulatory nature'.

9. In this context the experience of broadcast content regulation in the UK may have some value. While there is of course not a direct read across from highly regulated (and generally trusted) broadcast news to the current internet businesses, there are a number of lessons which might be of value in trying to create an effective regulatory or self-regulatory environment for the internet.

10. The first and most important principle of broadcast regulation in the UK is its commitment to freedom of expression. The Ofcom Broadcasting Code makes specific reference to the right to freedom of expression in Article 10 of the European Convention on Human Rights. It is quite possible, if very expensive, to censor the internet. China employs 2 million 'internet opinion analysts' to monitor web traffic and social media, and the government censors everything from disagreement with President Xi's proposal to

extend his presidency to any reference to Winnie the Poo after social media suggested some similarities in the physical appearance of the President and the bear.

11. Overall, social media and the internet have been a force for good in extending freedom of expression and making censorship and state control of information more difficult. The European Commission is clear that any new arrangements for the internet should strictly respect freedom of expression and avoid any form of censorship.

12. Three key elements of UK broadcast regulation may have some relevance to the search for effective regulation of news on the internet. They are agreed editorial guidelines establishing minimum standards; obligation on the broadcaster to deal with any mistake or complaint as speedily and effectively as possible; and a back-stop complaints procedure involving independent assessment when the complainant is dissatisfied with the broadcaster's handling of the issue.

13. Internet businesses such as Facebook and Google have their own versions of editorial guidelines, setting out the conditions on which they give contributors access, though they have tended to describe them as policies or community values. They are currently a long way short of the sort of editorial guidelines, which have been applied, to news broadcasters. The management of the main internet businesses has up to now been dominated by people with a technology or marketing background, though the companies have recently begun to recruit more people with editorial experience. Whether from their own resources or with help and advice from outside, they need to articulate more clearly what is and what is not acceptable in online news.

14. Equally important is the need to respond to justified complaints effectively and speedily. One of the advantages of social media is that feedback can be instantaneous. However if offensive or misleading material is not taken down quickly it can spread rapidly and the potential damage is far beyond the initial act of publication.

15. UK news broadcasters prioritise a rapid response to mistakes. When, on March 22 last year, Channel 4 News, in a rare mistake, identified the wrong man as the Westminster Bridge terrorist, the error was flagged on social media during the transmission of the programme. As soon as Channel 4 News realised its mistake, it corrected it on air and Channel 4 pulled the second transmission of the programme from its Channel 4 + 1 network. This could not completely undo the damage but ensured it was limited to that one transmission.

16. A consistent complaint about the social media companies is their failure to take down clearly offensive content as soon as it is flagged – or in some cases not at all. Improving their performance requires a significant shift in

management priority and the commitment of resources. Mark Zuckerberg told Congress 'By the end of this year; by the way, we're going to have more than 20,000 people working on security and content review, working across all these things. So, when content gets flagged to us, we have those — those people look at it. And, if it violates our policies, then we take it down'. He believed AI could identify 'certain classes of bad activity proactively and flag it'. The experience of broadcast regulation suggests that the best way to ensure that this works effectively is to set targets for speed of response and monitor performance against those targets.

17. The third key element of an effective system of regulation is some form of independent assessment of editorial guidelines and their enforcement through editorial monitoring and complaints handling. This can be an external regulator or an independent board – what matters is their competence and independence.

18. There is no doubt Ofcom could have an important role in exploring how far these ideas can be applied to the internet. However, it is currently in the anomalous position of only regulating some of broadcasters' online content. A first step would be for the government to give it responsibility for all broadcasters' content whether broadcast or online.

19. A second step could be to revisit the suggestion by Lara Fielden in her 2011 Reuters Institute paper Regulating **for Trust in Journalism**, that there could be tiers of regulation and self regulation, with the incentive of a 'kite mark' of recognition for those online news providers who agreed to a voluntary system of editorial standards and regulation below the current high level applied to public broadcasters but above the minimum legal requirements. The European Commission is also interested in the idea of improving credibility of information by providing an indication of its trustworthiness.

20. And Ofcom could also build on its excellent reputation for evidence-based analysis by commissioning research on what the public expect from the different sources of online new and what appetite there might be for different levels of regulation in the light of recent events.

21. In the field of broadcasting, the UK is at present the one of the most influential players in Europe. However its ability to influence the debate in Europe is likely to diminish after Britain leaves the EU next year. Ofcom will no longer be a EU regulator. And the UK's current role as the major broadcasting hub for Europe is also in doubt and subject to negotiation. As far as the regulation of the internet is concerned, a key decision for government will be how closely to align the UK with the EU in the future in these crucial areas of public policy where the global scale of both the issues and the companies involved suggests going it alone is unlikely to be as effective as working with strong international partners.

Professor Richard Tait – written evidence (IRN0042)

11 May 2018

Rahim Talibzade and Bishoy Maher - written evidence (IRN0015)

Transcript to be found under Bishoy Maherand

TalkTalk – written evidence (IRN0083)

Introduction

- Today, TalkTalk is the UK's challenger telecoms company, providing landline, broadband and TV 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 also by wholesaling to resellers.

- TalkTalk believes that technology companies have a responsibility to foster a safer online world. We are passionate about the benefits of the internet, but recognise that customers need support to navigate it safety. This should include helping customers to understand online risks, and ensuring products and services are designed with safety features to help mitigate them.

- TalkTalk is proud to have led the industry in rolling out products and services to protect families online. Examples include:

    - In 2013, we became the first ISP) to introduce free parental filters, putting parents in control of what content their children can access on all devices connected to the home wifi. All TalkTalk customers have now made an active choice about what level of protection their home requires. All new customers are also obliged to make an active choice as part of the sign-up process, but can modify and amend their settings at any point in response to changing family circumstances.

    - In 2014, TalkTalk helped to found Internet Matters, the not-for-profit child safety organisation dedicated to helping parents understand and mitigate online risks. We joined forces with BT, Virgin Media and Sky to pool resources and scale-up our efforts to promote online safety, and jointly committed £25m worth of support at its launch. Since its launch, Internet Matters has enjoyed considerable success:

        - Internet Matters' hub website has been visited 4.5 million times.

        - Over 200,000 teachers have visited the site and its education apps have been downloaded 21,000 times.

        - 80% of parents feel more confident handling issues after visiting the website.
        - 85% of users said they would recommend it to their family and friends.[1154]

[1154] https://www.internetmatters.org/about-us/impact-report-2014-2017/#1506342225860-7ce97a9a-464b

In 2017, all four ISPs committed to three years of additional funding for Internet Matters and are actively supporting it to scale to a wider audience, with a greater range of corporate supporters.

- TalkTalk has worked collaboratively with partners across the wider internet landscape to help tackle harms and promote positive online experiences. Action includes:

    - Membership of the Internet Watch Foundation, the independent organisation that works with the tech industry and law enforcement to identify and remove child sexual abuse images online. We are proud to be one of its largest funders and we also sit on its Funding Council.

    - We are members of the Royal Foundation's Taskforce on Cyberbullying and have supported its work over the past 18 months, including seconding members of staff to the organisation to help build consensus across the technology and charity sectors on action to better protect children online.

    - We have also supported wider efforts to increase digital literacy amongst adults and children to increase consumer confidence in dealing with the challenges of an online life, including funding the Good Things Foundation's digital skills initiatives.

TalkTalk – written evidence (IRN0083)

1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

Since its foundation in 2003, TalkTalk has worked with Government and industry on exploring and establishing the basis of internet governance and regulation. To date, this has been a self-regulatory approach with little statutory underpinning and has not involved an external regulatory body with broad powers. Instead, it has primarily featured industry-led discussions which have focused on reaching consensus and staying within agreed technological boundaries. These discussions have broadly all been guided by the principle of a light-touch approach to regulation, which sought to avoid third party interference in the relationship between connectivity / communications providers and its users wherever possible, preferring industry-led efforts. Throughout these discussions, TalkTalk has sought to champion the interests of consumers and has sought to represent the experiences and expectations of our customers.

This approach has been successful in many respects, with effective and swift industry action in response to emerging issues and public concern. Examples include:

- **Tackling child sexual exploitation online** – Founded in 1996 following discussions between Government, law enforcement and industry, the Internet Watch Foundation (IWF) operates a notice and takedown service to alert hosting service providers of such criminal content found on their servers. It is a self-regulatory body: it is member funded and membership remains voluntary; however, membership and compliance is almost universal across the British technology sector. It is governed by a board of 11 Trustees and a Funding Council, made up of members.

However, it relies on a legal framework to enforce its work: once informed of the presence of illegal content, the host or ISP is duty-bound under the E-Commerce Regulations (Liability of intermediary service providers) to quickly remove or disable access to the potentially criminal content. Its status as a relevant authority for reporting, handling and combating child sexual abuse images on the internet has been recognised in a Memorandum of Understanding between the Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) linked to Section 46 of the Sexual Offences Act 2003.

The success of this approach is clear: UK networks are some of the most hostile spaces in the world to the hosting of potentially illegal online content and confirmed reports of child sexual abuse content apparently hosted in the UK have reduced from 18% in 1996 to less than 1% since 2003.[1155]

[1155] https://www.iwf.org.uk/what-we-do/how-we-assess-and-remove-content/our-political-engagement/iwf-champions

- **Child-friendly filters** – In 2013, TalkTalk was the first ISP to introduce network-level filtering to block inappropriate content for children, and provide this service to customers free of charge. All TalkTalk customers have now been forced to make an active choice about whether to switch on our filters.

- Around 36% of new customers apply our filtering service, HomeSafe, at the point of sale, which is broadly proportionate to the number of UK premises with children. Other major ISPs followed our lead and now all four major ISPs offer these filters. At the request of the Secretary of State, Ofcom has produced regular reports analysing parental filters. These reports compiled comparable data on how filters operated; the categories of content covered; customer take-up; and complaints procedures. In its most recent report, Ofcom research found that more than nine in ten parents of 5-15s who use these tools consider parent filters to be useful, and around three-quarters say they block the right amount of content.[1156]

- **Net neutrality** – Since 2011, the Broadband Stakeholder Group has brought together ISPs, content providers and other interested providers, initially as signatories to a self-regulatory approach on traffic management practices. This evolved into a more wide-reaching Open Internet Code of Practice, which fulfils the requirement of the EU's Connected Content Regulation. This has proved to be effective: in 2017, Ofcom submitted a report to the European Commission on compliance with EU Regulation 2015/2120 on open internet access from May 2016 to April 2017 and concluded that "there are no major concerns regarding the openness of the internet in the UK".[1157]

These actions have been successful often because they have facilitated industry collaboration on issues which are widely recognised as requiring action. This shows how industry can react to clear problems in a nimble and effective way, establishing consensus in a swift manner, in the absence of regulation or legislation.

In contrast, some efforts to create new legislative and regulatory frameworks have proved difficult. After several years of discussion between industry and Government on protecting children from harmful content online, the Digital Economy Act (2017) introduced new statutory requirements for online pornography sites to implement age verification mechanisms, and will require ISPs to block sites which do not comply with the legislation. Having first been discussed as a policy option in the 2010-15 Parliament, the law was eventually passed in the 2017 Digital Economy Act and due to come into force in April 2018; however, the implementation date has been postponed and websites are unlikely to be blocked before 2019. This prolonged process demonstrates the complexity of the policy and the sensitivity around legislation on these issues. The new requirements are a significant change in internet policy in the UK and represents one of the first attempts to introduce

[1156] [https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf]

[1157] https://www.ofcom.org.uk/__data/assets/pdf_file/0018/103257/net-neutrality.pdf such legislation anywhere in the world. We therefore strongly welcome the Government's decision to delay implementation in order to consult more broadly with industry on the requirements and carefully consider the new processes which the legislation creates. This example demonstrates how a legislative approach to regulation is complex and may be a slower process than self-regulatory approaches.

Today's challenge

However, there are limits to the effectiveness of self-regulation. Despite the tangible, successful self-regulatory steps taken by industry, it is clear that harmful behaviour proliferates online:

- Research published in March 2018 which investigated young people's experiences online found that at age ten, girls who interacted on social media for an hour or more on a school day had worse levels of well-being compared to girls who had lower levels of social media interaction.[1158]
- In the year ending March 2017, two per cent (1,067 offences) of all hate crime offences had been flagged as having an online element.[1159]
- Research by OR and the NSPCC in 2017 found that:
    - One in three (1,194 out of 3,975) young people reported seeing violent and hateful content on online platforms;
    - One in five (815 out of 3,975) young people's reviews reported seeing sexual content including accidentally finding it, being sent sexual messages, or being encouraged to share sexual content themselves.
    - Just under one in five (772 out of 3,975) young people's reviews reported seeing bullying.[1160]

It is clear, therefore, that self-regulatory efforts have not resolved the full range of online risks. This is not surprising, given the pace of technology change, but it underlines the need to consider whether existing approaches are appropriate to deal with new and emerging issues.

Previous self-regulatory efforts have relied on industry consensus on the need for and broad principles of action. However, in the absence of this type of consensus, it is right to consider whether there should be outside efforts to introduce new

[1158] https://bmcpublichealth.biomedcentral.com/articles/10.1186/s12889-018-5220-4

[1159] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652136/hate-crime-1617-hosb1717.pdf

[1160] NSPCC (2017) Net Aware report 2017: "freedom to express myself safely": exploring how young people navigate opportunities and risks in their online lives. London: NSPCC.

regulation. Our position is that this is likely to require the formalisation and extension of new regulatory principles across the wider internet ecosystem.

An additional problem with the UK's fragmented and informal approach to internet regulation is the uneven way it applies across the internet industry. Discussions on internet safety initiatives are often focussed on large operators, with SMEs excluded from the process. For instance, discussions between industry and Government on parental filters were restricted to only 4 operators, with smaller ISPs exempted from any expectation to offer free tools to their customers. We accept that larger companies are more likely to have the resources to engage with such obligations, as well as the scale to reach large numbers of customers. However, this approach risks creating a two-tier approach to safety. The best way to protect families online is for companies to embed safety features in products from the outset. Excluding companies from safety obligations until they reach a certain size undermines that effort, and means companies that reach scale instead try to retrofit imperfect safety solutions onto existing products. That is often costlier and less effective.

The need for a more formally regulated, consistent approach has already found political and societal support. Most significantly, in December 2017, amendments tabled in the House of Lords to the Data Protection Bill introduced a new responsibility on the Information Commissioner's Office (ICO) to produce a statutory code of practice on age-appropriate website design. This new code will set standards required of websites and app makers on privacy for children under the age of 16 on issues such as:

- default privacy settings;
- data minimisation standards;
- sharing and resale of data;
- user reporting and resolution processes and systems.

These requirements will require transparency from online platforms and also require accommodation of regulatory standards. This offers a model for a future regulatory approach which would require platforms to conform to certain design principles (for example, having complaints and escalation processes that include particular features) and also require transparency about processes. Through these combined efforts, we believe that there will be both greater consumer understanding of the responsibilities and actions of online platforms. Moreover, transparency reporting provides an incentive on providers to correct known issues on their platform, and can also further the sharing of best practice across industry which can help other companies, particularly SMEs that may lack specialist safety resources or expertise, to adopt best practice quicker and more affordably.

There is a broader question about how these new requirements would be implemented, the legislative changes required, and what regulatory architecture would be required to oversee it - for example, to monitor compliance with regulatory standards and publish annual assessments on performance. This is not an easy question and is likely to be subject to much discussion and debate.

However, it is likely that there would need to be a regulatory body to oversee these requirements and act as an independent auditor of the platforms' compliance.

At present, we do not believe that there is a pre-existing model or body with the resources or knowledge to take on this responsibility. Future debate and consultation should set out different regulatory models and consider which is most appropriate. Regardless of which body would take on this responsibility, or whether it would be a new organisation, it is clear that its success would require it to have sufficient resource and powers to provide effective oversight and scrutiny.

We recognise this would be a significant step in the governance of the internet at a global level, and that there would be significant concern about possible negative impacts on both the commercial freedom of online platforms as well as freedom of expression. Therefore, it is clear that there needs to be significant public debate and consultation on the scope, extent and format of a regulatory body.

2. What should the legal liability of online platforms be for the content that they host?

The current approach to legal liability is a complex debate about the definition and purposes of platforms. It is specifically a legal debate which to date has had little crossover into consumer issues or discussions. However, this approach no longer seems fit for a world in which online platforms extend into different aspects of our offline life, and in particular as more and more young people use online platforms. This growing prominence of online platforms has led to increased consumer expectations of online platforms in recent years, with consumers wanting to see clearer communications and more consistent application of rules across online platforms. Therefore, the question of liability should reflect and respond to these discussions, and can provide the framework for a regulatory response.

The combination of increased expectations and unclear (and possibly outdated) liability rules has led to increasing confusion about platforms' roles and responsibilities. High-profile incidences of harmful or illegal content proliferating on platforms (or, indeed, the reverse problem of overzealous removal of content) due to uncertainty about what is required by the law, has led to a lack of knowledge and subsequent decline in trust in relations with tech companies.

More generally, there is a risk that consumer confusion and dissatisfaction is leading to negative perceptions about the role of social media in society: according to research for the YouGov-Cambridge Centre, just 14% of British voters think social media is ultimately good for society, compared with a striking 86% saying otherwise.[1161] This includes nearly half (46%) who believe social media has a negative effect on society overall, plus a further 24% who say the impact is

[1161] https://d25d2506sfb94s.cloudfront.net/cumulus_uploads/document/orlvgyfffb/YGC_Social_media_and_society_Jan_18.pdf "neither positive nor negative" and 16% who "don't know".[1162] Research has also found consumer demand for a new approach from social media companies: YouGov polling in 2017 found that 67% of people backed social media companies taking on the duties of publisher, rather than merely platform, in making sure that only genuine news stories are displayed onsite.[1163] Research in 2013 found people believe companies should be doing more to protect from bullying (72%) or harassment.[1164]

Therefore, TalkTalk believes consumer demand exists for clearer, more effective rules has increased and, therefore, that it is appropriate to reconsider the liability framework to provide greater clarity to consumers.

At present, the debate is focused on the division between responsibilities on publishers compared to platforms, which are designated as information society service provide under the E-Commerce directive (which is also TalkTalk's designation as an ISP). However, it does not appear to us that either of these categories are appropriate for online media companies: while in recent years they have moved away from acting as platforms to produce and curate content, this process is not comparable to those of a traditional media outlet.
It is possible, and likely, that a new category of liability will be required which recognises the new and evolving role of online platforms. Our positon is that this new category will recognise that it would be unduly burdensome to require them to authorise content pre-publication in the same way as a traditional media company, as this would not recognise the volume of content and also the relationship between platform and users, which is not comparable to that between a news editor and a journalist.

However, we believe that a new regulatory system – as set out in our response to Question 1 – could incorporate this new hybrid approach to liability. This would include placing a regulated responsibility on platforms to have processes and capabilities to react to concerns about content, and imposing certain minimum standards - for example requiring human moderation for reported content, or setting time frames in which content reviews need to be completed.

This new system will require a body to enforce these standards, which we have discussed in our answer to Question 1. As the designation comes as part of the E-Commerce Directive, it will also need to be incorporated into UK law ahead of withdrawal from the EU, as discussed in our answer to Question 9.

3. How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for

[1162] https://d25d2506sfb94s.cloudfront.net/cumulus_uploads/document/orlvgyfffb/YGC_Social_media_and_society_Jan_18.pdf

[1163] https://d25d2506sfb94s.cloudfront.net/cumulus_uploads/document/mn0dvlnx45/InternalResults_170309_FakeNews_W.pdf

[1164] http://cdn.yougov.com/cumulus_uploads/document/hoirf26dxl/YG-Archive-Pol-Sunday- Times-results-020813.pdf

individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

The scale of the task in content moderation cannot be overestimated: some 200 billion tweets are posted every year - or about 6,000 tweets per second[1165]; 300 hours of video are uploaded to YouTube every minute and a billion hours of content is watched every day on the platform.[1166] As technological capabilities and products evolve rapidly, governance and moderation systems often struggle to keep up.

We make three broad observations about the shortcomings of current moderation processes and areas where there could be improvement:

- **Delayed responses –** There is often a lack of urgency when it comes to enforcing community codes of conduct, which allows harmful content to be shared. This both creates immediate concerns about the wellbeing of those affected by the harmful content, and in the longer-term risks damaging public perception of the online world and its ability to identify harmful content and protect users.

- **Over-reliance on Artificial Intelligence –** Artificial intelligence (AI) has a role to play in moderating content, due to the scale of the task. However, the utility of AI is limited as it sometimes fails to view content in context, which is essential to understand whether it violates conduct rules. For example, recently YouTube was revealed to have allowed harmful comments under videos of family content.[1167] As the videos and the comments were moderated separately, there was a lack of overview which would have identified the potential for harm. This shows the potential difficulties from an AI first approach.

Moreover, companies are not always transparent about the extent of the role that AI plays in moderating content, and more transparency on this matter would help greater understanding about its capabilities.

- **Unclear rules –** The variation between codes of conduct in different platforms is to be expected. However, this variation often leads to confusion about what is and isn't acceptable. Platforms generally act to remove content which is clearly illegal (such as extremist content and hate speech). However, when content is clearly harmful but not illegal, there is often a lack of certainty about the companies' responses - for example, its reaction to cyberbullying or trolling. This lack of certainty is confusing for consumers to navigate, and also places pressure on online platforms as they plan their response to complicated cases.

[1165] https://blog.twitter.com/official/en_us/a/2011/200-million-tweets-per-day.html
[1166] https://youtube.googleblog.com/2017/02/you-know-whats-cool-billion-hours.html
[1167] https://news.sky.com/story/top-brands-pull-youtube-ads-over-paedophilia-fears-11141271

This problem is exacerbated by the fact that online platforms' terms and conditions, privacy policies and community guidelines are often long and complex pieces of text. Few consumers engage with them and it is difficult for even the most determined and capable of users to have a clear view of what is and is not acceptable conduct. Improving communication of these key policies should be a priority for online platforms, and we discuss possible improvement in our response to Question 6.

We support the recommendations of both the Royal Foundation's *Design for Safety Guidelines*[1168] and the UK Council for Child Internet Safety's *Child Safety Online: A Practical Guide for the Providers of Social Media and Interactive Services*[1169], which set out standards for online moderation systems, including:

- Easily understood behaviour policies with frequent reminders throughout users' journeys;
- A clear and transparent reporting process;
- Clear explanations of the consequences for misconduct online.

As referenced in our answers to Question 2, we believe there is a role for new regulation that will set minimum standards for platforms' moderation policies and also provide an independent audit process.

Reversal
There are likely to be instances when users object to platform's decisions about content moderation, and want to appeal the decision made. This shows the importance of building appeal mechanisms into any moderation processes.

However, platforms should retain freedom to remove content it deems to have broken terms of use and to be the ultimate arbiter in individual cases. This respects platforms commercial freedom. Moreover, it applies the same principle as in the offline world whereby member organisations manage and enforce member responsibilities. We do not believe there is a role for regulatory bodies in adjudicating in individual cases; rather, their role should be on overseeing and auditing the moderation processes.

4. What role should users play in establishing and maintaining online community standards for content and behaviour?

As we have outlined in our answers to Question 1 and 2, we believe that online platforms should be required to meet certain minimum standards when designing online community standards for content and behaviour. Companies should be required to demonstrate their compliance with the requirement on an annual basis

[1168] https://www.royalfoundation.com/wp-content/uploads/2017/11/Action-Plan_17115-1.pdf
[1169] https://www.gov.uk/government/publications/child-safety-online-a-practical-guide-for-providers-of-social-media-and-interactive-services/child-safety-online-a-practical-guide-for-providers-of-social-media-and-interactive-services

through new transparency reporting, and this compliance should be monitored or endorsed by an independent body.

Considering the role that users should play in this process, we believe that companies should engage users with community standards to ensure they are well-understood and considered to be an essential part of the platform. The Royal Foundation's 'Design Safety Guidelines' offer a good basis for building user awareness and validation of the community standards, including making sure the policies are written in plain language, that they are separated from more general terms and conditions, and also providing regular reminders of the policies (to reinforce their central role). Platforms should also emphasise individual accountability and responsibility for behaviour to users.

As we have stated in our answer to Question 3, online platforms should have ultimate responsibility for establishing and maintaining community standards for content and behaviour, providing that they comply with the requirements as set out by any new regulatory system.

However, while it is true that companies have ultimate responsibility for establishing and maintaining online standards, it is clear that users also have a role to play in maintaining community standards in their own regular use of online platforms. When they become aware of abusive or harmful behaviour, users should recognise that they have a responsibility to report these infringes of community standards. This is comparable to responsibilities in the offline world to challenge and report poor behaviour or practices. Online platforms should provide users with easy ways to report harmful behaviour and also give them the tools and language to challenge this behaviour where possible.

5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

As discussed in our responses to questions 1-4, we believe that online platforms should adopt the principle of safety by design and therefore adapt and reform platforms to build safety features in at this primary stage. This is similar to the approach adopted by ISPs in 2014 when they introduced family-friendly filters. In addition, companies have incorporated safe design features in products specifically for children: TalkTalk's Kids TV Remote was designed with input from school-age children, and keeps children's browsing within designated 'Kids Zone' with age-appropriate content and channels selected by parents, as well as the option of imposing time limits.[1170]

Online platforms have recently made welcome progress along these lines: recently, YouTube announced that its YouTube Kids app will be modified to allow parents to manually approve individual videos or channels that their children can access

[1170] https://help2.talktalk.co.uk/about-kids-tv-remote through the app, giving them the ability to pre-vet and handpick a collection of videos to ensure they are appropriate.[1171] This progress is welcome; however, it should go further and faster. The Data Protection Bill offers the opportunity to research and develop new safety features, and the overarching regulatory system will enable the sharing of best practice more broadly across the industry.

We accept that this is a complex and evolving landscape, and we are also mindful of concerns about freedom of expression. However, we do not believe these changes will increase the risk to freedom of expression. Rather, clearer rules around content moderation and more transparency about platforms' decision-making processes will be beneficial in increasing public awareness about platforms' moderation policies, as well as its broader relationship with users in relation to data etc. Platforms will no longer set and impose their own terms of engagement with no external accountability, but instead will operate within a regulatory system whereby its responsibilities are clear. In this way, there will be greater oversight of moderation decisions and any perceived encroachments on freedom of expression can be challenged in public.

6. What information should online platforms provide to users about the use of their personal data?

Recent media coverage demonstrated the gap between how online platforms use personal data and users' own expectations of data handling. Many users have been surprised by the extent to which their data is collected, the time for which it is stored and how it has been shared with third party companies.

This points to a general problem of low levels of engagement with data protection issues and poor user understanding of how data is processed and handling. We believe that there are several reasons for this circumstance, and many of these are applicable to consumer experiences in different sectors. However, online platforms' direct and frequent contact with their users gives them a particular ability to improve their communication and trial different ways of increasing engagement and awareness. We believe there is more that could be done to make their data arrangements and privacy agreements easier to understand – for example, using clearer language. Furthermore, many platforms already prompt users to review privacy settings on a regular basis. We think this approach should be extended to all platforms and should be put on a more regular and structured footing – for example, implementing bi-annual privacy checks which require users to actively re-commit to their data and privacy settings.

The Department of Business, Energy and Industrial Strategy's *Modernising Consumer Markets: Consumer Green Paper*, published in April, states that "consumers rarely read terms and conditions" and highlights online platforms as a particular new challenge for consumer protection, concluding that "now that

[1171] https://youtube.googleblog.com/2018/04/introducing-new-choices-for-parents-to.html consumers' data is commonly being collected by online companies in exchange for 'free' goods and services, consumers need to understand what they have agreed to when accepting a contract or privacy notice."[1172] As part of this policy agenda, the Behavioural Insights Team will produce a concise, good practice guide for business on presenting terms and conditions and privacy notices online. This process will involve randomised control trials to test which forms of communication consumers find most comprehensible and will be informed by behavioural science techniques. We are encouraged by this work and believe it can play an important role in increasing consumer awareness about terms and conditions more generally, and believe it has particular relevance to this discussion around data protection and privacy in an online environment.

In addition, as discussed in our previous answers, we strongly support the amendment to the Data Protection Bill to require the ICO to produce guidance on processing children's data and believe that this additional responsibility must be implemented in full by all online platforms, including SMEs and new companies.

7. In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

As a commercial company, we appreciate the principle of commercial confidence, and accept that this principle can come into conflict with the transparency demands of a regulatory regime. However, commercial confidence cannot be used to avoid calls for further transparency. As discussed in questions 1-4, we believe that greater transparency about content creation and moderation policies is required to improve standards across the board and increase consumer understanding of the system. We support the Government's plan to introduce a transparency report through the Internet Safety Strategy and hope it helps improve transparency in the industry. We also support the Data Protection Bill's introduction of a statutory code of practice on age-appropriate website design, and believe that these requirements will improve transparency of online platforms' broader business practices.

Moreover, we do not believe that this requirement of additional transparency is overly onerous or detrimental to online platforms and therefore do not see why they should not comply with proportionate and well-structured transparency requests. Other media and connectivity companies are subject to transparency requirements to operate in the UK. Ofcom has a statutory right to request information from ISPs, including TalkTalk, that guarantees Section 135 of the Communications Act 2003. This information contributes to Ofcom's market review processes and also its broader responsibilities to review competition in the sector. Information requested can cover future investment plans, product launches and technology development. Failure to provide the information in a timely manner or to provide accurate information can lead to substantial fines imposed on ISPs:

[1172] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/699937/modernising-consumer-markets-green-paper.pdf earlier in 2018 an ISP was fined £70,000 for failing to provide accurate information in response to a request related to the Wholesale Local Access market review.[1173]

Beyond this information which will be included within the Data Protection Bill requirements and the transparency report, we also support industry efforts to increase transparency in advertising on online platforms. In common with many other major brands, TalkTalk places advertisements on online platforms and welcomes this opportunity to engage with potential customers in a targeted and personal way. However, we would like to see more transparency about this commercial arrangement, specifically around the placement of advertisements on user-generate content, the identification of target audiences and the use of metrics to monitor and measure advertising content. This would bring this form of advertising in line with offline advertising and would help build confidence of major brands.

8. What is the impact of the dominance of a small number of online platforms in certain online markets?

As a challenger brand, TalkTalk believes that effective competition delivers the most efficient and effective markets, and is imperative to protect consumer interests. Online platforms have had a disruptive impact and have fundamentally transformed several markets – for example, online streaming platforms have transformed content distribution and, increasingly, content creation in the audio-visual sector.

However, as online platforms begin to consolidate, concerns about competition in this sector have grown.[1174] Economics tools have been understandably slow to adapt to the features of online markets and therefore analyses of competitive forces have been constrained. As online platforms look to monetise their consumer reach through advertising, market power comes from access to large data sets. As this market becomes more and more concentrated, it could act as a barrier to entry for new entrants and instead the market could stagnate, delivering poor results for users.

We note the Lords' Communications Committee's recommendation that the Government reviews whether competition law is appropriate for the 21st century digital economy, and also that the CMA investigates the digital advertising market to ensure that it is working fairly for consumers and other businesses.[1175] In addition, we support the Department for Business, Energy, Innovation and Skills' *Modernising Consumer Markets: Consumer Green Paper*'s focus on consumer protection in online markets and support efforts to bring greater transparency, and

[1173] https://www.ofcom.org.uk/about-ofcom/latest/bulletins/competition-bulletins/all-closed-cases/cw_01208

[1174] Coyle, D (2017): https://www.ft.com/content/9dc80408-81e1-11e7-94e2-c5b903247afd; Duch-Brown, N (2017): https://ec.europa.eu/jrc/sites/jrcsh/files/jrc106299.pdf

[1175] https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/116/116.pdf the work the CMA is currently undertaking to understand more about consumer experiences of online businesses and platforms.

9. What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

Much of the current regulatory architecture is determined or influenced by European regulation, including the E Commerce Directive which determines the online liability regime; the Connected Content Regulation on net neutrality and the European Electronic Communications Code. At present it is our understanding that these laws will be transposed into UK law through the EU (Withdrawal) Bill and therefore there should be no significant disruption.

However, questions remain about how future divergence will be managed, and it is important that there is clarity on the UK's approach to this throughout the transition period and afterwards. The global nature of online platforms means that international actions will be important to monitor and respond to, and it is likely the UK will need to be mindful of the European Union's approach to these issues when designing its own regulatory systems and processes.

May 2018

TalkTalk Group, Sky and Virgin Media – oral evidence (QQ 103-112)

Transcript to be found under Sky

Dr Damian Tambini, London School of Economics and Political Science – written evidence (IRN0101)

Background evidence provided for oral evidence session of Tuesday 1 May

How to negotiate with platforms

After a series of scandals about Facebook in particular, but also YouTube (Google) and other platforms, governments are now involved in multiple negotiations with powerful Internet intermediaries. But the danger is that these complex processes will get bogged down and Parliament and the public will be played by the platforms. In order to ensure the best deal for the public, Parliament and the state need overall strategy and coordination, and genuine support of the public.

With the House of Lords and the House of Commons select committees now running parallel Inquiries into fake news and Internet regulation, the platforms have finally been dragged to the table. What happens next in Brussels, Washington and London will shape not only the Internet but the traditional media, for generations. The emerging crisis has occurred because these info platforms now play a crucial infrastructure role in most of our lives. Therefore they are too important and powerful to ignore. They are associated with a range of harms from hate speech to child exploitation to social media dominance in advertising markets. They enjoy power without responsibility as news publishers, widespread data tracking in surveillance capitalism supported by addictive behaviours, and are re-engineering our built environment from the High Street to our transport infrastructure. But they also deliver huge benefits, which is one reason why it is so difficult to leave.

Such a broad impact requires a more far-sighted approach: Policymakers must consider more holistic approaches to the problem of platform power. This means 'joining up' the various policy fields where states and platforms are negotiating about the responsibilities of the platforms. If policymakers fail to do this, they will undermine their negotiating position.

The House of Lords Inquiry poses the question of whether 'the internet' should be regulated. Whilst fascinating as a provocation it is the wrong question. As Harvard Law professor Cass Sunstein long ago pointed out, regulation is the norm on the internet, as property rights, and protection from harm is necessary online as it is elsewhere. The regulatory question is how and by whom. The internet – as a regulatory object – is difficult to grapple with, because it is nothing but a cluster of communications protocols and standards. What does exist, and what increasingly is controlling and even supplanting the internet for many consumers and services, is platforms and intermediaries such as Google, Amazon, Facebook and Apple. This is what the Inquiry is really about. If we, via our representatives do not regulate the platforms, they will regulate us.

A Prior Question: What is the social value of platforms?

The government has a standard procedure when considering if anything needs to be regulated, and that is the treasury's Green Book. According to this government bible, policymakers must first ask whether markets will fail to deliver optimal welfare. Like the methodologies used in competition law, it is based on a model of individual consumer welfare. As pointed out by myself and colleagues here, there are limits to this approach when it is applied to complex, incommensurable policy issues. Fundamentally, the value to society of matters like broadcasting and the internet are not possible to capture in simple models based on cash values. But nonetheless, in policy terms, what is the value of a service to society is the question that must be asked before any regulatory question is posed; whether that is the question of whether something needs regulating at all (the Green Book) question; or how? Through fiscal measures, competition instruments or some form of licensing. In the context of BBC regulation, there is a generally accepted – if sometimes contested – notion that the BBC delivers positive social externalities – or public value - that would not be delivered by the market. Our problem with regulation of the internet is that we have not even asked the prior question of whether the internet – or rather the platforms - deliver social value or whether that value might be negative.

The truth is of course that what the platforms do is being worked out in a discussion across society and Parliament. That is what we are doing: Parliament is negotiating with the platforms –as it did previously with the press - about how and to what extent they will serve society, and what regulatory deal they will get to facilitate this. The problem is that until now, this has been done in a fragmented way across different areas. The solution to the current impasse is not going to be a tweak here or there, but a policy response that is coordinated across multiple policy areas. Competition policy - shaping and structuring the market as a whole - must be considered alongside other forms of regulation. If this process fails, Parliament and government have many options. These include at the extreme breakup or nationalisation of platforms or punitive regulation. China and Russia have demonstrated that the structure of the internet does not prevent licensing controls of social networks. In liberal democracies that recognise fundamental rights the regulatory solution will involve autonomous institutions, regulated in the public interest, but the detail of how regulation will work institutionally (what combination of self, co- and statutory regulation) are yet to determine. Government must rediscover the social objectives behind regulation and develop a clearer vision for where they want to get to. This means negotiating a new 'social compact' for the platforms, which respects their autonomy, but gets the balance right between transparency, independence and accountability.

Tax

Fiscal policy can be used to achieve social policy goals. There is a consensus in favour of high taxation on tobacco and alcohol, gambling and sugar, because of the overwhelming evidence of individual detriment and negative social externalities associated with consumption of those products. On the other hand tax breaks are offered to goods considered beneficial, for example, controversially, all newspapers in the UK benefit from a VAT exemption. Because they provide virtual services, there has been a history of ineffective enforcement and taxation of the platforms, and a degree of avoidance. As a result there has been a lot of discussion of using fiscal policy to achieve regulatory outcomes, but not a great deal of decisive action. This is due not only to difficulties of enforcement but because there is no consensus on the social benefits or costs associated with for example social media, search or the wider data and AI services they enable.

In recent weeks and months this consensus has shifted: in part because of the growing realisation that data driven 'surveillance capitalism' may act to the detriment of individual well-being, and fundamental rights including privacy; and in part because new evidence has emerged about worrying negative political and social consequences of platforms, including in the most sensitive areas of elections and national security. These negative externalities are particularly difficult to assess: there is currently a very wide range of opinion on the cultural, political and economic benefits – and dis-benefits delivered by platforms.

In such an environment, calls for levies on platforms to fund various social goods including news gain more traction. Policymakers in France and Germany have developed several iterations of digital taxes already, and US expert Victor Picard recently called for a "public media tax" on Facebook and Google's earnings to fund public interest journalism. He calculated that a 1% tax on their 2017 net income in the US alone could yield $285 million for independent journalism. A similar proposal has been advanced in the UK by campaigns such as the Campaign for Media Reform. The hazards of such an approach are obvious – the compromise of genuine independence, but the history of the BBC and other policy instruments demonstrate that it is entirely possible to provide public funding and protect media independence.

What would it mean to 'break up' Facebook or Google?

Martin Moore and I conclude our book with the call to 'open up or break up' the dominant social media platforms. We are by no means the first to advocate this obvious move. Emily Bell, one of our chapter authors has made the same point. With companies that have the economic features of network effects that lead to 'natural monopolies' the choice, as summarised by Taplin over a year ago is whether to regulate them as monopolies or break them up. Experts such as LBS Professor and former Which Chair Patrick Barwise are now of the view that the economic properties of platform markets are such that normal processes of competitive creative destruction may not work: data driven dominance enables social media to become entrenched and see off competitive entrants. We are therefore currently at a decision point. Breakup or regulate as monopolies? Breakup is the 'big stick' held in the background as a discussion goes on about what kind of regulation might work.

What kinds of structural separation would address the public policy concerns?

If it does come to breaking up platforms how would that work? This is not science fiction. Various forms of structural separation remedy are available in communications regulation, BT has over the past decade been required by Ofcom to progressively disengage its wholesale from its retail division, and classically the history of US anti-trust has shown that both with regard to the energy sector and in relation to communications with the breakup of AT+T, regulators and Congress have been prepared to break up unacceptable concentrations of economic and political power when this becomes necessary. All the signs both from Brussels and Washington are that momentum is building for such a break up. This could take the form of a *separation* between the different operations of the platform company, for example between the advertising, personal data, content production and user generated content aspects of a given company. (Discussed further below). And if a structural solution cannot be found, regulators can shape behaviour. One could imagine a public interest intervention requiring some form of divestment or structural separation combination of, petition and public interest concerns after the existing enterprise act, but this would in all likelihood require new legislation.

How does competition law need to change?

A related issue is the fact that existing competition law and anti-trust has been developed and applied in a way which creates difficulties in dealing with concentrations of market power in platforms. There are various problems: one is that consumer interests are often constructed in narrow terms and in particular in relation to price. Lina Khan points out in her excellent essay that Amazon's long-term strategy of achieving market dominance through low price, while sacrificing short and medium term profits has had the additional benefit to Amazon of providing good deal of immunity from competition law as it appears to regulators that Amazon's low prices indicate the degree of consumer benefit. Martin Moore's work makes clear that the history of anti-trust in the US is a history in which competition law and regulation has much wider social objectives than price alone. Whilst there is a need for a good deal of caution in offering regulators or politicians wide discretion in examining the public interest benefits of private actors such as Internet platforms, it is entirely possible to design regulatory systems that ensure regulated companies protect a wide range of public benefits. Drawing on the history of media regulation in particular, and the combination of sector specific public interest benefits with general competition benefits it should be possible to arrive at new forms of regulation.

Real Transparency and Access to Data

Academics have called for access to data and more transparency with increasing militancy. Most recently participants at the conference in Amsterdam and more recently in Perugia have demanded better access. Regulators, to need to know more about the process of opinion formation. This inevitably raises questions about the autonomy and independence of Internet publishers and would require legal and constitutional restraints under the European Convention on Human Rights. Facebook recently announced that it was setting up or facilitating the setting up of an independent body - a council of academics and civil society representatives that would be granted access to data. Although this is a useful delaying tactic for Facebook it is difficult to see how it will work in practice: given commercial and personal confidentiality such a body could not be granted unfettered access to Facebook's systems and they would ultimately be in the position of making requests for data to Facebook, and data could be formatted as Facebook requires. This is no substitute for the kind of statutory body with licensed access to private data within clearly defined terms, as advocated by US experts such as Frank Pasquale.

Redefine Platforms as media?

Journalists are fond of calling for a level playing field between Internet intermediaries and news media and in particular calling for the redefinition of platforms as publishers. What this would mean in practice is to change the liability structure for Internet Intermediaries, something previously regulated from Brussels. Culture Secretary Matt Hancock recently announced that the Government would be consulting on this, as the UK could develop its own policy post Brexit. This is not a new issue. Back in 2011 the Council of Europe called for a "new notion of media" in which Internet publishers would assume many of the responsibilities and obligations of media and also benefit from privileges and exemptions enjoyed by media. Whilst this kind of policy shift is attractive in principle, in practice it may be an immensely complex affair particularly in the United Kingdom where there is no overarching definition of what a publisher in fact is. In France and Germany there is more clarity regarding the obligations, for example of transparency that pertain to publishers in general. There is a consensus building on both sides of the Atlantic that the very wide exemptions and immunities granted to Internet intermediaries are not sustainable and provide an unfair subsidy to the platforms. The question is; what to replace it with. How hard to be on the platforms?

Tough GDPR implementation for social networks?

The platform business model is essentially based on exploitation of personal data. They can offer smarter advertising, and a range of ancillary services because they know more about you than their competitors do. But personal data regulation is being tightened, and how this is carried out, particularly in Europe has the potential to shift the dial on whether their business model works. The GDPR will be in force across Europe from the end of May 2018. This is a major paradigm shift in the regulation of social networks, and regulators will face a number of decisions in relation to how to exercise considerable discretion they have in implementing. How they do so will depend in part upon what range of complaints they receive, and the wider policy discussion around platforms is bound to have an impact.

Campaigners fought hard for a right to data portability, they did so with social networks very much in mind. But in practice and effective right to data portability will depend on a range of interpretations: will it in fact be possible for you to download your entire Facebook history, photos, friends, delete them from Facebook and transplant them into a competitor social network? That is the policy solution that would fuel real competition, but it is one that Facebook and co will fight tooth and nail to prevent.

Protecting Democratic Legitimacy

Election Laws also need to be radically reformed. Part of this is about having spending limits that are easier to enforce and would prevent the kind of money laundering, shell companies and benefits in kind that are alleged to have occurred in relation to the referendum and part of it is about new offences relating to deliberate attempts to mislead voters through targeted advertising. Some have called for outright bans on political advertising in social media: this may be going too far as there are likely to be significant benefits to various forms of targeted communication.

In the longer term we need to have a debate about propaganda. It was the rise of totalitarianism in the mid-20th century that gave rise to the paradigms of media freedom and media pluralism protection within the Council of Europe system. The rise of artificial intelligence and data driven algorithmic propaganda pose new challenges not merely at the level of new centres of powerful corporate authority, but at the level of each individual citizen whose autonomy is challenged by the ability of propagandists to know and understand their identities interests their intimate ideas and behavioural proclivities. The platforms have an important role to play in this: but what they do matters to all of us. It is not acceptable for monopoly players, or even big players in oligopolistic markets, to enjoy the role of censors and editors without transparent ethics and accountability.

Copyright

One of the key bones of contention between platforms and news publishers is the extent to which platforms are able to exploit news created by others for advertising revenue. One of the things that states can do is pass laws which alter the balance of power between publishers and platforms. The European Union’s current proposals for a ‘press publishers right‘ is one such proposal. What they would do is introduce another layer of protection, in addition to existing copyrights and database rights, by creating a very broad right of ownership in news. Such proposals would however create significant negative outcomes: for example by undermining the free flow of quality news and ideas, and arguably creating space in the market for ‘fake news’. In redesigning the copyright regime Parliament is effectively switching the dial that determines flows of revenues either to publishers or to platforms. But they are doing so without a debate about which of the two deliver real social value. The Fake news issue is a smear with which traditional media can daub the platforms, but let’s not forget that the press are not perfect, and a broad swath of the UK press is currently acting in a contemptuous attitude to Parliament and its Royal Charter.

What about Brexit?

Many of these proposals have a European dimension: there is no doubt that it would have been easier to coordinate a powerful EU-wide response without Brexit. A coordinated EU response makes it more difficult for the platforms to shift their activities around according to the most conducive legislation, thereby creating a race to the bottom as states compete to host the platforms. But there are reasons to be optimistic that European cooperation and collaboration could continue regardless of what kind of Brexit, if any, is achieved. Many of the proposals are well underway at an EU level. The GDPR has been more than a decade in the making, and the UK is committed to implementing it. The digital single market proposals are more of a grey area, but the signals are that if anything the UK government wishes to be more tough on the platforms than our EU neighbours.
One of the ironic and indirect impacts of Brexit is that the role of bodies such as the Council of Europe, which sets human rights standards for a much wider area, become more important as companies and governments seek to avoid inefficient balkanisation. Recently the Council of Europe set out's new principles for the regulation of intermediaries. These and other standards of the Council of Europe will likely have more impact with a shift of emphasis from the European Court of Justice to the European Court of Human Rights.

What does all this mean for "Internet freedom"?

We have come a long way since the late and recently lamented John Perry Barlow made his celebrated declaration of the Independence of Cyberspace in 1996. It was Hillary Clinton in 2011 who made the key intervention in defining the new US doctrine of 'Internet Freedom.' The platforms themselves have, as one might expect embraced this notion for their own self-interested objectives, for example claiming that intermediary liability shields, and protection from various forms of transparency obligation are crucial to freedom of expression. It is certainly the case that opposition and dissent in authoritarian countries can benefit from free Internet services including global access, but it is also the case that Internet freedom, like press freedom needs to be understood as instrumental - i.e. as conditional on serving particular democratic ends - and institutional - that is as implying a certain social responsibility with regard to the institutions of democracy. Internet freedom, like the other freedoms of communication, is by no means absolute. Individual human rights of freedom of expression will continue to be claimed and defended online as well as off-line. Internet platforms, particularly those that enjoy monopoly or dominant positions are likely to operate as censors or pseudo-censors through their ability to block, filter, or make more prominent certain forms of content. So it is time that the communicative gatekeeping role of Internet players was regulated and regularised alongside those of other publishers. The maintenance of a separate regime for Internet only players is unsustainable.

Dr Damian Tambini, London School of Economics and Political Science – written evidence (IRN0101)

How to Manage Reform? What should the Parliamentary Inquiries do?

Macho phrases like “open up or break up” should rightly raise the hackles when one considers the longer history of media freedom. We do not want the government kicking Facebook’s doors down, any more than we want them smashing printing presses or Guardian laptops. This is why process matters. If any single party or government of the day attempts to design the constitutional settlement for platforms history tells us they will not be able to do so without attempting to create a media system tilted in their own favour. Almost a century ago when the new medium of radio was in its infancy, the Sykes and the Crawford committees set out the framework for the policies that would establish the BBC. These were independent commissions involving parliamentarians along with other experts. Such processes were laughably elitist of course, but as a basic model that involves, but is not limited to Parliament, it remains the way forward. There must be an independent Committee of Inquiry to investigate platforms, and this should cover not only regulation, privacy, and child protection, copyright, fake news and hate speech but the entire range of issues where the role of platforms, not of the ‘internet’ per se are raised. The House of Lords is a great place to start, but the process needs to be more open, more civil society led, and more plugged in to the huge range of international initiatives in this space.

The ‘open up’ part of the deal must mean being subject to data transparency requirements to regulatory institutions that are independent of the state. Facebook’s recent announcements that they will create data access for academics is not enough. There is an opportunity for Facebook and Google to set some global standards here. Whilst the reality of the state in China or Iran for example would not permit genuine independence, working through institutions such as the global net initiative, the platforms could develop a framework for revealing data to genuinely independent third sector bodies with oversight of civil society and academia, which would not compromise rights to freedom of expression and privacy in the context of state oversight.

As this process of negotiation unfolds, it is crucial to have a clear and shared notion of the wider citizen interests that are at stake. Politicians need to decide whether, for the purposes of tax and competition law, Facebook is more like tobacco, or more like public broadcasting. In many ways the UK is coming to the party late: other countries have been involved in trying to operate in a more fundamental constitutional level: Brazil passed a constitution for the Internet in 2014. But the Brazilian authorities have had difficulties enforcing these abstract laws without a firm grounding in constitutional traditions and the support of civil society. They also, frankly lack the global authority that the UK enjoys as a long-established working democracy. So it is worth asking at this stage how such a negotiation between states and the powerful global platforms can work. The platforms, and particularly Facebook now accept that they are not only powerful monopoly players but they are powerful monopoly players playing an important social role in society and as such should be subject to various forms of social regulation. They do not want however to be subject either to rules that do not meet global norms of human rights nor do they want to be subject to a complex patchwork of rules in different markets. Until now there has been no credible threat of global regulation. The existing global institutions, such as the Internet Governance Forum and other bodies that work under the UN umbrella simply don't have the enforcement power required and operate as talking shops and coordination mechanisms. The first step must be taken by national parliaments, and the UK is well placed to do that. But the current approach of multiple overlapping Inquiries resulting in uncoordinated tweaks to regulation here or there cannot continue. An independent cross party commission established by Parliament should now address the platforms with one voice, and a clear message. The debate about the overall social value of the platforms is prior to the multiple overlapping questions about how they should be regulated.

One option might be to re-open what the Royal Charter on the Press Might be for. The government are at an impasse, but they have already created a valuable legislative and regulatory machine in the recognition panel and the incentives of the Crime and Courts Act. Perhaps one role for such a Commission should be to redefine what it is for, and make sure that it deals with a wider range of social ills- and social benefits – delivered by this new breed of platform publisher. Whatever the content of the eventual deal, it is clear that the first proposal must be for a vehicle that is up to the task of carrying out a multi-year negotiation with the platforms and to do so with a credible threat of the full range of policy tools, competition, fiscal and regulatory, that Parliament can ultimately call upon.

How to "Break Up" Facebook[1176]

A first stage could be behavioural rules designed to separate out different functions within the company. These are one way in which specific social objectives are baked into competition law in order to deal with potential negative consequence of market dominance. An analogy is the public interest test for media mergers.

In the Enterprise Act (2002, s58) there is a specific public interest test which is applied in the case of media mergers. The test gives ministers powers to attach conditions to mergers. These are the powers which underlie for example the undertakings being suggested by those companies bidding for control of Sky. Ofcom and the Competition and Markets Authority have both agreed that there is a specific public interest that relates to the continuation of quality independent news provided by Sky News. Therefore the 'suitors' wishing to purchase Sky have offered commitments firstly to continue funding Sky News, and secondly to maintaining its independence for example through separating the management of Sky News from the rest of the company.

[1176] Previously published on the LSE Media Policy Blog, as: http://blogs.lse.ac.uk/mediapolicyproject/2018/05/02/how-to-break-up-facebook/

These public interest rules relate to a specific historical period in which News and particularly broadcast news has played a hugely important role in society. They were developed over a long period of time, and apply also in mergers involving newspapers, for the same reason. These rules, along with self-regulatory ethical codes, and ethical practices such as the separation of editorial and advertising, form an important part of a regulatory system for the news media that protects against concentrations of unaccountable power and propaganda.

The rise of platform power raises a number of additional social objectives which are reflected neither in the legislation, nor in the guidance offered by regulators. These have included foreign interference, hate speech, misinformation, election offences, and use and abuse of personal data for targeting purposes. Facebook and other dominant platforms are developing ethical principles and practices – analogous to the separation of advertising and editorial – to regulate their own services, by designing in ethics, but they may need help from civil society to work through this wide range of issues. One way that the Inquiry could encourage platforms to work harder to develop their ethical practices would be to examine what forms of internal structural separation might ensure a more ethical Facebook. Ultimately, these could be written into a public interest test but the first stage would be self-regulation.

Separate advertising and editorial?

One proposal could for example be to separate advertising from what we could call the 'editorial' functions. (Curation of newsfeed and relevance algorithm). Many of the problems associated with Facebook in recent years relate to this function within the company, for example opaque targeting, proto-censorship, advertising-funded propaganda and hate. Might it be possible for Facebook to operate a strict internal separation between advertising and editorial, as has been the case in powerful news media for approximately a century? This could be done on a voluntary basis, but some co-regulatory oversight by a regulator would help.

There are lots of precedents for separating editorial functions from advertising, and not only in newspapers. UK public broadcaster Channel Four was originally prevented from selling its own ads, to protect the public service nature of its output from commercial imperatives. If Facebook was able to separate ad sales and newsfeed, it would be more free to develop its own ethical algorithm in ways that benefit society, and not only its shareholders.

A New Institution

This negotiation, to be effective requires a new institution: if Facebook (or other dominant platforms) do not develop their own ethical separations of functions, in the way that newspapers and others have developed their own approaches to these fundamental ethical questions, then some of this might have to be enforced by a regulator. We are currently having a societal debate about the ethics and responsibilities of platforms like Facebook but the discussion is fragmented, there is no ‘credible threat’ of regulation or breakup that will ensure that such companies deliver on their responsibilities.

The government’s Digital Charter process lacks transparency, independence, and public involvement. Historically, through for example Royal Commissions on the press, and broadcasting policy commissions, there has been a convention that major matters of policy which impact media freedom and autonomy will be dealt with through commissions that are independent of government with a transparent set of terms of reference and a clear process. The Digital Charter is driven by a safety agenda, which is hugely important but only part of the regulatory challenge of platforms. The process, which is run by the government, is not transparent or consultative. There is no guarantee this process will be continued by any future government. (The Opposition for example has plans for its own Charter).

We need a new institution that is capable of articulating to dominant platforms the broad range of societal interests in their operation, developing sensible ways in which they can be addressed and monitoring the extent to which principles are adhered to. This should not in the first instance be a ‘regulator’ and it will not license social networks, but it should set out objectives of regulation which could be implemented by platforms and report on their implementation. It should be able to monitor transparency reports and audit self-regulation. If separation between advertising and editorial on platforms works is agreed as an objective, and works on a voluntary basis, breaking up the company through law (which would likely require involvement of the EU or other countries) would not be necessary.

This institution must be independent of the government of the day and must be able to advise Parliament whether it would be necessary to use the full range of tools: in fiscal, competition and other forms of regulation to encourage more public-interest oriented behaviour on the part of platforms. If Facebook intends to maintain its dominant position in the social media market, it has a responsibility to work with Parliament and civil society to ensure it serves all our interests.

These themes are explored more fully in the edited collection:
Moore, Martin and Tambini, Damian (eds).
Digital Dominance: The Power of Google, Amazon, Facebook and Apple.
Oxford University Press, May 2018.

May 2018

techUK – written evidence (IRN0086)

Executive Summary

1. techUK represents over 950 tech companies, ranging from global tech firms to fast scaling new businesses. The majority of techUK members are small and medium enterprises (SMEs).

2. While we acknowledge the public policy concerns that underpin this inquiry, we are concerned by the vague nature of some of the questions being asked as part of this call for evidence. The issues are numerous and complex, and it is important that the committee embraces this complexity in order to improve understanding of the issues being discussed.

3. 'The Internet' is not a single business model or activity. It is a complex ecosystem made up of many different layers, players and business models. As such, references to regulating "the internet" are not helpful, and a more specific and accurate approach should be taken.

4. There are some legitimate concerns about the development of the digital economy, however it is important that the complicated and diverse ecosystem is properly understood before proposing legislative changes that could have wide-ranging and unintended consequences. Crucially, there is much within the current legal framework that offers an appropriate basis for effective action to be taken to address specific concerns and we invite the committee to identify the frameworks that work and should be safeguarded. We expand on this in more detail below.

5. The idea that 'the internet' is an unregulated 'Wild West' is inaccurate. Activity which takes place online is subject to the same rules, laws and standards that operate offline. In some areas these standards may not be fully adapted to the digital age and new training and guidance is required to ensure effective enforcement of current laws. However, the principle remains and techUK wholeheartedly support the Government's ambition to preserve and strengthen this principle.

6. Online intermediaries are not free of any liability for the content they host. The current law sets out specific circumstances where online intermediaries have limited liability, and these are specific to the activity they undertake in the digital ecosystem. The current framework is technology neutral and independent of business models.

7. There are a range of legitimate issues the committee is looking at. However, this is a highly complex ecosystem and clarity is needed on the problems that we need to address. Broad consultation is needed on potential remedies.

There are real problems of focusing on intermediary liability as a broad-based solution for a complex range of concerns. It would be better to look at specific and targeted solutions. Given that these can be achieved in the current legal framework it is likely this would be a faster route to the positive outcomes the committee seeks.

8. The UK's withdrawal from the European Union should not be seen as an opportunity to re-write the foundations upon which the UK's successful digital economy has been built. To do so would lead to reduced innovation, conflicting rights and freedoms and markets that are less open to entry by UK entrepreneurs.

About techUK

9. techUK welcomes the opportunity to provide written evidence to the House of Lords Communications Committee on the topic of internet regulation. techUK is the trade association for the UK technology sector, representing over 950 businesses. Our members range from leading FTSE 100 companies to new innovative start-ups. Collectively they employ more than 800,000 people, about half of all tech sector jobs in the UK. The majority of our members are small and medium sized businesses.

Introduction

10. The UK's digital economy is the envy of much of the world. It is estimated that the UK's 'digital sector' accounts for 16 per cent of domestic output, 10 per cent of employment and 24 per cent of exports[1177]. The UK's digital economy has been able to flourish due to an innovation-friendly environment and a clear and predictable regulatory structure. Far from being a the 'wild west', as it is sometimes suggested, the internet operates based on a set of complex, interdependent rules, laws, industry standards and self/co-regulatory codes. This provides targeted governance to address specific issues which allow new services and products to develop that provide significant benefits to consumers, citizens and society. The e-Commerce Directive has been a long-standing, core foundation of this legal framework and has been fundamental to the growth of the UK's digital economy.

11. It should be noted how vast the scope of this inquiry's call for views is. 'The regulation of the internet' is an issue which covers an almost endless list of topics and activities, and the committee should be wary of inadvertently creating different standards for online and offline activities. To flip the question, if we were to be talking about the regulation of the offline world this would be a cross-governmental response encompassing all areas including schools, hospitals, the environment, health and safety, banking and everything in between.

[1177] https://www.techuk.org/insights/news/item/10086-the-uk-digital-sectors-after-brexit

12. As we will discuss there are some legitimate concerns about the development of the digital economy, however it is important that the complicated and diverse ecosystem is properly understood before proposing legislative changes that could have wide-ranging and unpredictable consequences. Legislation is not always the answer. Given the dynamic and ever-changing nature of the digital ecosystem non-legislative initiatives between government, industry and civil society offer more appropriate and effective mechanisms for meaningful and successful action. A good example is the Intellectual Property Office's Code of Practice on the removal of copyright infringing websites in search results[1178]. Another excellent example is the world leading Internet Watch Foundation (IWF) which, due to its self-regulatory model, has been able to successfully adapt and keep pace with rapid technological change.

13. We urge caution in reviewing the legal liability provisions for intermediaries under Directive 2000/31/EC (ECD) and its UK implementation, the Electronic Commerce (EC Directive) Regulations 2002. This framework has been a founding principle of regulation that has underpinned the development of the digital economy.

Q1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

14. This is a poorly framed question which risks eliciting confusing responses that will be unhelpful to the task of understanding how and what regulation should evolve. Firstly, it refers only to the internet when we assume the intent is to also include the world wide web and the myriad of services that are enabled by and operate over the web. The internet and the web are enablers of a huge range of activities – commercial, non-profit and individual – most of which are entirely positive and benign.

15. The internet and the web must be understood as a complex ecosystem made up of many different layers, players and business models. As such, using 'regulation of the internet' as 'short-hand' to talk about how specific problems in the online world can be addressed is unhelpful. A more specific and accurate approach should be taken that is led by evidence and is clear about the different layers and actors within the internet stack. For example, the roles and responsibilities of infrastructure providers and those responsible for the "public core" of the internet are very different to consumer-facing platforms which organise content. Furthermore, a broad range of businesses operate "platforms" of some description, but these are not always intermediation platforms, or consumer-facing platforms.

[1178] https://www.gov.uk/government/news/search-engines-and-creative-industries-sign-anti-piracy-agreement

16. Secondly, it should be noted clearly that the activities the internet allows to take place are already subject to the same laws that apply offline. The Government's ambition is to create an environment where consumers "have the same rights and expect the same behaviour online as we do online". This is a principle that techUK wholeheartedly agrees with and believes exists already. For example:

    - the Companies Act states that products and services must have accurate descriptions;

    - the Consumer Rights Act requires businesses to treat customers fairly;

    - advertising rules to protect consumers are the same for off- and online adverts;

    - online content is regulated by the same standards as offline when it comes to hate speech, although there is no specific definition of hate speech; and

    - abuse through email or instant messaging, for example, is already an offence under the Malicious Communications Act 1988.

17. These requirements are subject to active enforcement in the online world, as they are in the offline world. Often what is missing is guidance and training to those charged with enforcing the rules. This can be achieved through improved training and guidance, adapted for the digital age. Additionally, it should be recognised that this is a partnership where Government, public agencies and industry can work together to address the challenges faced.

18. Finally, this call for evidence should be clear about the problem to be addressed, rather than starting with a solution without a clearly defined problem. Clear definition of problems will enable better focused and practical approaches. We would remark that this call for evidence is focused on specific interventions. These may be inappropriate for some or all stakeholders and may have unpredictable and unintended consequences on the vibrancy of the digital economy. We are experiencing a period of rapid change in technology and user habits which means new legislation, if aimed specifically at 'the internet', may also simply be ineffective.

19. There are perfectly legitimate concerns about the nature of certain types of content found online and action being taken to remove inappropriate content. It is right that there is a public debate about the best way to address those concerns. However, we must be specific about those concerns in order to find solutions that work.

20. Policy makers should take a technology-neutral approach which involves multiple stakeholders, builds on existing laws, improves training and guidance for a digital age, avoids blunt legislative instruments and recognises current

voluntary and co-regulatory efforts. Achieving this is as much an offline issue as it is an online issue. There should be a greater understanding of how online platforms and apps work so that, when citizens interact with them they can do so in a resilient manner. Government, industry and civil society all have a role in achieving this. The committee should also be open to recommending international collaboration where issues are best addressed in partnership with other governments or via global initiatives.

21. Much of the discussion as centred around the minimum legal obligations relating to liability of content. However, companies often complement the law. The Royal Foundation Taskforce on the Prevention of Cyber-bullying is a clear example of this. Companies have supported the 'Stop Speak Support' campaign which has created an online code of conduct to help children feel empowered to question online behaviour, speak out and support their friends. These types of initiatives are possible and have been developed through the existing legal framework. Amending the legal requirements risks putting companies off these initiatives for fear they may cut across new law.

22. To this end, techUK recommends that the committee adopt some guiding principles that will:

- Commit to a forward-looking and pro-innovation approach
- Be led by the evidence and specific and detailed problem definitions
- Adopt a bias against regulatory intervention and for collaborative action
- Follow a technology-neutral approach which does not favour any specific technology or business model over others
- Be robust in examining impact of any interventions on wider ecosystem
- Put the needs of consumers at the forefront of considerations

Q2. What should the legal liability of online platforms be for the content that they host?

23. The question of what the legal liability of online intermediaries should be for content they host is a complicated one. It is often suggested that intermediaries have no liability for the content they host. This is simply not the case and is a misunderstanding of the legal framework in which online intermediaries, of different types, operate.

24. The current regime, based on the e-Commerce directive, balances a range of interests. This is not just in the interests of the intermediary involved but it also enables a balance to be struck between the rights of everyday users,

holders of rights including creative and expression rights, victims of offences and other groups.

25. Crucially, the current regime is activity based, not platform or business model based, so where a limitation to liability exists it applies to a specific activity, not all activities. It also overlays other law and legal obligations so any changes to the liability regime would have a knock-on effect on other areas of criminal and civil law. Finally, there are other areas of regulation and self-regulation applying to digital, which is linked with the liability regime, meaning there could be further knock-on effects from changes, such as the CAP Code on Advertising Standards[1179].

26. It is important that the committee appreciates the full range of intermediary activities which fall within the scope of this regime. Through case law, including cases in the UK, the framework encompasses not only regular hosting, but more sophisticated activities like professional discussion boards, university networks, sports fan forums and the increasingly social and immersive offerings of the creative industries: virtual worlds, augmented reality, multiplayer online games and so on. Domain name registrars, security platform services and other crucial activities are also impacted. Changes to the current liability regime would therefore have wide ranging and significant impact on supply chains right across the digital economy.

27. Some intermediaries manage their own content, some intermediaries host user-uploaded content. Indeed, many intermediaries will do both. Therefore, the type of content hosted, and the liabilities attached to hosting it, will be different across different types of intermediaries. To be clear, hosting is the activity, while the intermediary is the part undertaking that activity.

28. Under the e-Commerce directive intermediaries have limited liability if:

- content appears on their platforms for which the intermediary only provides certain technical functions and has no editorial control

- they do not initiate the transmission or modify the content, along with other specific legal requirements.

- they act expeditiously to remove or disable access to content once they have received actual knowledge of illegal activity or information. If they do not act expeditiously they will not retain the limitations to liability.

29. This final point has led to the development of notice and action systems which provide intermediaries with a framework to take action on illegal content where they have actual knowledge. Providers are responsible and liable for content which they either produce or 'make available' and have actual

[1179] https://www.asa.org.uk/codes-and-rulings/advertising-codes.html knowledge of. They would therefore not be considered an intermediary and subsequently not benefit from limitations to liability.

30. The current approach to intermediary liability has allowed a huge diversity of intermediaries to become established and grow and provides previously unimaginable opportunities for people and businesses to access new markets. Attempting to insert barriers to the sharing of content will have an inevitable freezing effect on innovation and distribution channels for creators and businesses. Putting full liability for user-uploaded content onto intermediaries would put those intermediaries in a significantly more uncertain position and would increase risks. Intermediaries would have to manage the legal risk coming from hosting user-uploaded content which would limit their ability to operate. This is particularly true for start-ups who are unlikely to have the resources available to mitigate such risks.

31. There are a number of challenges with amending the current liability regime. First, as has been mentioned already, the liability framework overlays specific laws. Identifying how and at what point an intermediary knows that content is illegal is not straightforward. Courts would determine this in the offline world and companies should not be the arbiters of what is considered illegal speech.

32. Secondly, there is a live discussion about what obligations intermediaries should have to intervene in the supply chain and the knock-on effects for established public policies. This discussion needs to consider where proactive action is appropriate. For example, the interests of a free press are not served if online intermediaries in the distribution chain have independent rights or legal duties to intervene and control content. Additionally, the use of technology to automatically remove content may result in speech rights or fair use rights being over-ridden.

33. Ultimately, putting full legal liability for content onto intermediaries would lead to such intermediaries being forced into becoming arbiters of what is acceptable and what is unacceptable. This would also have widespread implications on rights such as the freedom of expression and freedom of information. There would be an understandable propensity for intermediaries to be over-cautious to avoid risks and therefore limiting availability of content that is perfectly legitimate, leaving intermediaries in a complicated legal situation. This was highlighted in a recent case in Germany where following the introduction of The Netzwerkdurchsetzungsgesetz (NetzdG) (German Hate Speech Law), Facebook took action to remove the posts of a user but was then told by a German court it was wrong to do so[1180]. It should be noted that the NetzdG law did not transfer liability to the intermediary but introduces significant fines for a failure to act. This chilling effect could have untold consequences on the availability of legitimate content. The balance achieved

[1180] https://www.bloomberg.com/news/articles/2018-04-12/facebook-told-to-stop-deleting-german-user-s-immigrant-comment by the current liability regime must therefore be maintained to avoid such conflicts. It should be for Governments or independent bodies to make such decisions, and for businesses to then comply and act to remove illegal content, as they do now. Clearly, there is scope to improve the speed and effectiveness of current approaches which would be a better focus for policy makers than seeking to change the overall approach to limitations to liability.

34. The committee has the opportunity to embrace the detail and complexity of the issues being discussed and to recognise the value of the current framework in balancing rights and responsibilities online, while focusing efforts on promoting initiatives which address the identified problems which government and industry has a shared interest in tackling.

Q3. How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

35. Whether platforms should proactively seek out illegal content is a complex technical, legal and operational issue. Internet companies may wish to act responsibly and take steps to tackle certain activity on their service but where this touches on the rights of others or complex areas of law, they do so at some legal and reputational risk.

36. Only a small number of the largest platforms would be in a position to do this yet experience tells us that the most successful actions against online harms (such as the IWF) are the result of collective action across the ecosystem, including by smaller and less resilient companies. Thus, we would encourage the committee to consider how ‘good Samaritan’ defences can provide confidence for companies across the digital ecosystem attempting to take good faith action in grey areas of the law.

37. In addition, the sheer scale of many online platforms would mean that only the largest could put in the processes and technologies to actively monitor content. Imposing obligations on all would serve as a significant barrier to entry for new platforms. Even relatively new online platforms can have significant scale, while larger ones such as YouTube have 400 hours of content uploaded every minute, and Twitter have over 500 million tweets a day[1181].

38. While liability is limited for online platforms these limitations can only be enjoyed if the intermediary acts expeditiously to remove illegal online content upon request. Therefore, when a notification is made this sparks a process of

[1181] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/home-affairs-committee/hate-crime-and-its-violent-consequences/oral/75919.pdf moderation where a decision must be taken whether to take down the third-party content in question or not.

39. techUK recognises that there are concerns about specific types of online content. Here clarity is needed about the specific type of content in questions so specific solutions can be delivered around it. For example, there is no legal definition of hate speech in the UK, which makes moderation of this type of content incredibly difficult. Once clarity is achieved it is more achievable for companies to develop mechanisms to tackle specific content online. The IWF is an example of this in action, where problems can be tackled in a collaborative way when there is clarity over both the type of content in question and what is considered to be unacceptable. The committee should also consider the role of state institutions in the moderation of online content. For example, the Director of Public Prosecutions has provided guidance on how existing law applies to social media posts which has provided a helpful deterrent to users and helped the police bring offenders to justice, as well as helping providers take their own action.

40. The largest digital platforms invest significantly in people and technology to ensure this moderation process runs smoothly. It estimated that more than 100,000 people are moderating content globally - from violence, hate speech to child sexual abuse - in addition to the algorithms being applied to this process.[1182] In addition, Facebook recently announced it would grow its moderation team to 20,000 staff in 2018, with Google announcing it would also have 10,000 people working on the moderation process by the end of the year[1183].

41. As AI technology develops it is becoming possible for some firms to identify suspect content automatically – often before it has been viewed by the platform's users. A significant amount of content which has already been removed or identified is now automatically blocked before upload with thanks to AI. Microsoft recently published 'The Future Computed'[1184] which looks at the potential uses of AI, along with ethical and legal considerations of this technology. However, manual reviews are still necessary in more complicated cases in order to make the finely balanced judgment as to where the appropriate balance of rights lies. This is what a court would do in the offline world. There is no company able to replicate courts' breadth of legal expertise and judgment, and government does not expect this of any other business sector. Another approach for the most complex areas of law is clearly necessary. This is an issue that the Committee should look into in detail as we do not want to end up with different standards and values applying online than offline and this will have consequences for the type of internet British consumers enjoy.

[1182] https://www.accenture.com/t20170901T024331Z__w__/lv-en/_acnmedia/PDF-49/Accenture-Webscale-Content-Moderation-POV-V2.pdf

[1183] http://fortune.com/2018/03/22/human-moderators-facebook-youtube-twitter/

[1184] https://blogs.microsoft.com/uploads/2018/02/The-Future-Computed_2.8.18.pdf

42. The challenges facing those tasked with moderating content online are numerous and global. They must take into account local laws setting different standards and fragmenting the 'global communities' being created.

43. There are clear pitfalls in seeking a greater role of content moderation – and censorship, for private businesses. This draws them into the field of policing freedom of expression and given the dangers of getting it wrong we are seeing businesses erring on the side of caution. There is also a question of definition. The role the internet has played in allowing human rights defenders and dissenting voices to promote their message, communicate and organise has been well documented; these groups can be documented as 'terrorist organisations' by some actors, and striking the balance is not straightforward or static. Lists of designated terrorist organisations usually form the starting point but there have been numerous incidents where entire accounts have been suspended incorrectly.[1185] This exemplifies the minefield we are asking organisations to operate in, and as set out above it would be inappropriate for private companies to be the arbiters of what is considered appropriate content.

Q5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information.

44. Our response to question two sets out our view that the current legal regime for platforms balances the rights of freedom of expression and information with the responsibility to ensure that illegal content is removed. It should be noted that the rights of freedom of expression and information are fundamental rights which apply in the offline world. If there is a suggestion that these rights should be treated and applied differently in the online world, this would merit are much deeper consideration as to the potential impacts and we urge the committee to be mindful of the risk of establishing greater restrictions online than would be considered acceptable offline.

45. With regards to online safety, companies frequently participate in campaigns and initiatives to ensure that their online communities are safe spaces. The UK Council for Child Internet Safety's recent guide for providers of social media and interactive services includes examples of good practice from leading technology companies, and advice from NGOs and other online child safety experts to encourage 'safety by design'. It has six key principles: Managing Content on Your Service; Parental Controls; Dealing with Abuse/Misuse; Dealing with Child Sexual Abuse; Privacy and Controls; Content and Illegal Contact; Education and Awareness.

[1185] https://www.theguardian.com/technology/2017/jun/06/facebook-chechnya-political-activist-page-deleted

46. The government's initiative in the Internet Safety Strategy to provide small start-ups and app developers with more information to ensure that they can "think safety first" and build in safety measures is a welcome measure.

47. Crucially technological tools should not be treated as a panacea, or allow them to diminish the role of parental engagement and education. Online platforms should provide parents with information and advice on how to keep their children safe online e.g. through Internet Matters, funded by industry, the online portal that provides safety advice to parents to keep children safe online.

Q6. What information should online platforms provide to users about the use of their personal data?

48. The United Kingdom has had a long tradition of strong data protection laws from the Data Protection Act 1984, through to the Data Protection Bill is currently making its way through Parliament to implement the EU General Data Protection Regulation.

49. Technology companies take data protection incredibly seriously given the importance to tech businesses of personal data and the link between reputation and trust. New data protection laws, which take effect on 25 May 2018, set out very clearly the responsibilities all organisations, including platforms, have when it comes to protecting personal information. This includes detailed requirements on Subject Access Requests which allow data subjects to request information that an organisation holds about them. This information must be provided to the data subject within one month of receipt of the request.

50. Transparency about how an organisation uses personal data is a key principle of GDPR and should be taken seriously by all businesses. This transparency should go beyond complicated language in Terms and Conditions and ensure that the data subject knows how their information is being used. This is a key in building trust and confidence in the way data is used. It is only through building confidence and trust that the benefits and opportunities of a data-driven economy will be realised.

51. These new data protection laws represent the most significant reforms to data protection in over twenty years. Given companies have been investing heavily to become compliant with the new law from 25 May 2018, now would not be an appropriate time to revisit data protection requirements. It is also not yet clear exactly what effect GDPR will have once it takes effect as case law is likely to have an impact.

Q7. In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

52. As techUK said in our submission to the House of Commons Science and Technology Select Committee inquiry into Algorithms:

> *"Key to building a culture of trust and confidence in automated decision-making systems is ensuring decisions are auditable, challengeable and ultimately understandable by humans. Clarity on what is meant by transparency, openness and accountability will also be key and the false perception that decisions made using algorithms cannot be challenged and are unfair must be addressed.*
>
> *However, public trust and confidence won't be achieved by legally requiring companies to publicly open up algorithms; which are likely to be commercially sensitive and unlikely to be understood by people without the appropriate technological knowledge. Instead ensuring the right mechanisms are in place so organisations and individuals can challenge the outcome of automated decision-making systems should be the focus of this discussion."*

53. An additional point to note is that as Artificial Intelligence technologies develop the issue of explainability will become more important. It is important that people understand how algorithms reach their decisions. Transparency, education and explainability are all linked.

Q9. What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

54. Much of the current legal framework in which technology companies, including online platforms, operate in originates from European law, and the EU has taken a more active interest in some of these issues through the Digital Single Market initiative. The impact of leaving the European Union will be significant. Given the global nature of the internet it will still be important to align regulatory efforts with the EU given the volume of trade that is facilitated between the UK and EU by online platforms.

55. When it comes to data protection, techUK has been clear that the UK should maintain alignment with the EU on data protection issues[1186]. There has been some suggestion that the UK might use Brexit as an opportunity to diverge on data protection to make it easier to strike trade deals with other countries, such as the US. techUK believes this is unnecessary and inappropriate. A key priority for the tech sector in Brexit negotiations is securing the free flow of data between the UK and EU through mutual adequacy agreements. The UK Government has rightly committed to implementing GDPR in full and will seek an ongoing role for the UK Information Commissioner on the European Data

[1186] https://www.techuk.org/insights/opinions/item/12291-why-tech-companies-don-t-want-the-uk-to-diverge-on-data-protection

Protection Board. This is an important step to securing an adequacy agreement and one which techUK supports. As the Prime Minister set out in her Munich speech, regulatory alignment is the right starting point and regulatory divergence would come at a cost which would need to be carefully assessed on a case by case basis.

56. The Prime Minister stated in her Mansion House speech that the UK would be leaving the Digital Single Market. It will be important to monitor developments in the EU's Digital Single Market as it will continue to affect businesses operating in the UK. The current liability framework, outlined above, is derived from the EU's e-Commerce directive. On 19 March 2018 the Secretary of State for Digital, Culture, Media & Sport told Parliament '*With Brexit, we will of course be leaving the e-commerce directive, so it is not a question of updating it, but of what to put in its place.*'[1187]

57. techUK welcomes the Government's commitment, via the Withdrawal Bill, to maintaining alignment with all EU digital regulation including the eCommerce directive. We would urge caution in attempting to re-write the e-Commerce directive in the short term, given how it has served as the underpinning legislative tool for much of the digital ecosystem. The committee has an opportunity to consider the full consequences of changing this for all the entities, as outlined in this response, that fall within scope of the current regime.

58. There is no one-size-fits-all to the issues being raised about online content and amending the e-Commerce directive would have serious unintended consequences. Any intervention must be highly targeted and take into account the wider implications. Government also need to more clearly define the problem they are attempting to solve, to ensure the right solutions are find. The UK's withdrawal from the EU should not be used to fundamentally re-write the rules of the internet without a full appreciation of the knock-on consequences.

Conclusion

59. techUK welcomes the opportunity to respond to this inquiry, which covers a fundamental part of the modern economy. We have set out the guiding principles we believe the Committee should take as it conducts its inquiry. Crucially, it is vital that the Committee notes the complexity of the digital ecosystem and the internet's role within it.

60. An approach which brings together government, industry and users, building on existing laws and efforts to ensure everyone can be safe online, which is

[1187] https://hansard.parliament.uk/Commons/2018-03-19/debates/2015B5CE-9F99-4B8D-B195-57C51AB4FD0C/CambridgeAnalyticaDataPrivacy#contribution-106ABD2B-2751-4760-BDDB-8C43ED14565D flexible to the changing nature of technology and user-habits is far more likely to succeed than a sharp legislative action.

May 2018

techUK and Coalition for a Digital Economy (Coadec) – oral evidence (QQ 44-51)

Transcript to be found under Coalition for a Digital Ecomony

techUK - supplementary written evidence (IRN0112)

Q9. What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

1. Much of the current legal framework in which technology companies, including online platforms, operate in originates from European law, and the EU has taken a more active interest in some of these issues through the Digital Single Market initiative. The impact of leaving the European Union will be significant. Given the global nature of the internet it will still be important to align regulatory efforts with the EU given the volume of trade that is facilitated between the UK and EU by online platforms. Failure to do so could create a situation where companies are required to operate under two different regulatory structures in order to service both the EU and the domestic market. For many businesses, particularly smaller tech firms, the cost and complexity of having to operate in this way may mean choosing which market to serve, thus limiting potential for growth and exports.

2. There are numerous areas in which divergence with the EU risks making the regulatory landscape more complex. One of the most important areas is data protection. techUK has been clear that the UK should maintain alignment with the EU on data protection issues[1188]. There has been some suggestion that the UK might use Brexit as an opportunity to diverge on data protection to make it easier to strike trade deals with other countries, such as the US. techUK believes this is unnecessary and inappropriate. Data protection is important in ensuring that UK citizens can be confident that their data will not be misused or treated without the appropriate care. Maintaining alignment on data protection is also important economically as, without it, UK businesses would not be able to transfer data between the UK and the EU or hold EU citizen's data. That is why a key priority for the tech sector in Brexit negotiations is securing the free flow of data between the UK and EU through mutual adequacy agreements. The UK Government has rightly committed to implementing GDPR in full and will seek an ongoing role for the UK Information Commissioner on the European Data Protection Board. This is an important step to securing an adequacy agreement and one which techUK supports. As the Prime Minister set out in her Munich speech, regulatory alignment is the right starting point and regulatory divergence would come at a cost which would need to be carefully assessed on a case by case basis.

[1188] https://www.techuk.org/insights/opinions/item/12291-why-tech-companies-don-t-want-the-uk-to-diverge-on-data-protection

3. In addition to data protection, there are other key elements of EU law that underpin the way in which the internet operates, and which make up the Digital Single Market. The Prime Minister stated in her Mansion House speech that the UK would be leaving the Digital Single Market. It will be important to monitor developments in the EU's Digital Single Market as it will continue to affect businesses operating in the UK. The current liability framework, outlined above, is derived from the EU's e-Commerce directive. On 19 March 2018 the Secretary of State for Digital, Culture, Media & Sport told Parliament '*With Brexit, we will of course be leaving the e-commerce directive, so it is not a question of updating it, but of what to put in its place.*'[1189]

4. techUK would urge caution in attempting to re-write the e-Commerce directive, given how it has served as the underpinning legislative tool for much of the digital ecosystem. The committee has an opportunity to consider the full consequences of changing this for all the entities, as outlined in this response, that fall within scope of the current regime.

5. It is also worth noting that, many elements of the Digital Single Market are themselves evolving. For example, there are still discussions within the EU as to whether to see to amend the e-Commerce directive during the next European Commission. There is therefore a risk that regulation, for example on limitations to liability, in both the UK and the EU could be changing at the same time, but in different ways. This is likely to cause significant confusion and complexity to business.

6. There is no one-size-fits-all to the issues being raised about online content and amending the e-Commerce directive would have serious unintended consequences. Any intervention must be highly targeted and take into account the wider implications. Government also need to more clearly define the problem they are attempting to solve, to ensure the right solutions are find. The UK's withdrawal from the EU should not be used to fundamentally re-write the rules of the internet without a full appreciation of the knock-on consequences.

7. Finally, it is important to note that, post Brexit, it is highly likely that UK citizens will continue to be able to access content from websites hosted across the world. This already presents a challenge in regulatory terms as it is difficult to enforce penalties on websites owned and hosted outside of Europe. That is why the tech sector has long supported efforts to deliver regulation at a global level, which

[1189] https://hansard.parliament.uk/Commons/2018-03-19/debates/2015B5CE-9F99-4B8D-B195-57C51AB4FD0C/CambridgeAnalyticaDataPrivacy#contribution-106ABD2B-2751-4760-BDDB-8C43ED14565D ensures compliance in all countries. Attempts by the UK to regulate the internet after the UK leaves the EU may therefore be easier to achieve at a legislative level, but substantially harder to enforce. Regardless of the Committee's view on the value of changing the way in which the internet is regulated, techUK believe it is important to consider the challenges that diverging with the EU in these areas will create in terms of securing the outcomes regulation is intended to create.

July 2018

Thinkbox – written evidence (IRN0056)

Who is Thinkbox?

1. Thinkbox is the marketing body for commercial TV in the UK – in all its forms and using all technologies including the internet. We represent over 99% of TV advertising revenue and our main shareholders are Channel 4, ITV, Sky Media, Turner Media and UKTV, though we also enjoy support from many broadcasters and TV platforms in the UK and around the world.

2. Thinkbox has a strong, legitimate interest in this topic. TV companies have always used every new technology that has appeared to distribute their channels and programmes; they have put much investment into delivering TV online through their VOD (Video on Demand) services, and internet technologies might one day replace broadcasting as the main TV technology. It is crucial therefore that the structure, ownership and regulation of the internet – both content and advertising – is fair, competitive and in the public interest.

Summary

The main points we would like the Committee to consider are as follows:

3. The internet is a global, public asset, like the air and the oceans. Just as we have laws that stop harmful emissions into the air or the sea, so we can and must regulate the companies that organise, provide access to and manage people's access to content and services online.

4. This won't prevent all bad behaviour online by individuals or rogue and criminal groups, but it will stop any reputable company from breaking important laws. We shouldn't be deterred by our inability to prevent all law-breaking; we aren't deterred in any other sphere of civic life and we can bail out a lot of water with a leaky bucket.

5. Internet companies and platforms should take full legal responsibility for all the content that they host. They, through their services and brands, provide the interface with the public and this brings responsibilities that they must accept in the same way as other media.

6. Internet platforms often claim that the task of vetting all of the content that they host is impossible as there is just too much of it. They publish and apply their own standards and offer to respond to complaints by removing illegal or offensive content post hoc. But by then much damage has already been done. The scale of the task of pre-vetting is only proportionate to the size of their

businesses. They have a choice not to accept all and any content and/or to charge fees for hosting content.

7. People should have a right not to be tracked and then, even if they consent to be, not have their personal data shared with any other party without their express, informed consent.

8. The 'dominance of a small number of online companies' that the Committee identifies in its Call for Evidence is not a situation that would be tolerated in any other market, at least not without paying some sort of monopoly tax. It is making it very difficult for other media companies that rely on advertising – as the so-called digital duopoly of Google and Facebook do – to move their businesses online, whether this be newspapers, magazines, radio or TV services. This is a threat to UK culture and democracy and we welcome the recommendation in the Committee's recent report on 'UK advertising in a digital age' that the Competition and Markets Authority should investigate the online advertising market to ensure it is working fairly for consumers and other businesses and whether current competition law requires change.

'The internet'

9. The word 'internet' derives from the 'interconnected networks' of computers, which digital technology has enabled. The internet is not the only 'digital' technology of course; all computing based devices, including cameras, watches, DVDs and CDs, are digital, not to mention all TV broadcasting and growing levels of radio broadcasting in the UK. For this reason, it is better to avoid using the word 'digital' when we specifically mean the internet.

10. The internet has two distinguishing characteristics: 1) its connectedness or interactivity, the two-way nature of communications that enable activity to be tagged and tracked, and 2) its global footprint as national boundaries (or regulations) cannot be enforced easily.

11. A network of connected computers needs an operating system to manage it; the world-wide web, an open and free software, was the most ubiquitous system but in recent years more closed, proprietary systems have been developed such as mobile apps, and these are now preferred by many tech companies.

Questions set for the inquiry

Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

12. It is useful to look at the TV industry as an example. TV is regulated by Ofcom and adheres to the highest standards. The moment it slips below those standards it provokes public outcry and can be subject to punitive measures. But this is incredibly rare because regulation is proven to work. TV has a proud

record as a well-regulated industry. Internet companies are not held to anywhere near the same standard as TV. They are not bound by the same rules – nor, indeed, are they subject to the same taxation. As it stands, the broadcasters' hands are effectively tied twice: first by having to adhere to much stricter regulation and second by paying a more equitable level of tax. As Google, Facebook and other online media owners begin to have greater ambitions in commissioning TV-like content to compete with TV for advertising investment there is a legitimate case to be made for greater equalization.

13. It has often been said that it is impossible to regulate the internet; that it is too unwieldy, amorphous and intangible. One could just as easily say that we cannot regulate the air or the oceans; we cannot stop thunderstorms nor tsunamis yet we do have laws which establish how companies should behave in relation to the air and oceans. We set standards of behaviour through laws and prosecute those who flout them. This is how we should think about the challenge of regulating the internet; we can and must regulate how the companies that organise, provide access to and manage people's access to content and services online. This won't prevent all bad behaviour online by individuals or rogue and criminal groups, but it will stop any reputable company from breaking important laws. We shouldn't be deterred by our inability to prevent all law-breaking; we aren't deterred in any other sphere of civic life and we can bail out a lot of water with a leaky bucket.

14. It is not unreasonable to believe that a lack of adequate internet regulation partly explains why there have been so many high profile transgressions of social and ethical norms by some internet companies in recent years. It is surely in the public interest to want greater oversight to help prevent future transgressions. Despite the damage to some companies' reputations – and indeed to the reputation of and trust in online companies more widely – little damage has been done to their bottom lines so perhaps there is little incentive for them to change.

15. The internet has enabled many wonderful things to develop, giving easy access to knowledge and communication to many more people around the world. But we should not be blinded by these benefits into accepting that the anti-social behaviour and harmful developments it has also facilitated are inevitable.

16. There is an ideology that grew up with the internet which rejects the idea of any attempt to regulate it on the grounds of restricting freedom of speech. We acknowledge that there is genuine idealism behind some of these pronouncements but, sadly, that idealism can and has been exploited as camouflage for criminal behaviour (e.g. identity fraud, terrorism) and more ruthless and land-grabbing instincts from corporations. The internet is a global, public asset, like the air and the oceans. No company should try to own it or prevent access to it by erecting its own barriers and entry points.

What should the legal liability of online platforms be for the content that they host?

17. Tech companies and platforms should take full legal responsibility for all the content that they host. They, through their services and brands, provide the interface with the public and this brings responsibilities that they must accept. The normal rules of publishing should apply. It is not like the private, closed communication that occurs through email, phone conversations or even chatting in a pub, though even in these situations we have laws that prevent people, for example, defaming others or promoting hatred.

18. How much worse is it to offer a public, heavily marketed platform, where people can distribute illegal and offensive content, with a search engine that makes it easy to find and even with a mechanism for monetising the content in some cases? Society would not tolerate such a thing if it were in any other sphere.

19. In many instances, illegal activity online is driven by the ability to generate advertising money. By requiring advertisers not to support online companies which do not abide by internet regulation, UK regulators could use one of the most effective levers available to it.

How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

20. Internet platforms often claim that the task of vetting all content that they host is impossible as there is just too much of it. They publish and apply their own standards (e.g. on nudity) and offer to respond to complaints by removing illegal or offensive content. But by then much damage has already been done.

21. The scale of the task of pre-vetting is only proportionate to the size of their businesses. They have a choice not to accept all and any content and/or to charge a small fee for hosting content. Many internet platforms boast vast profits from which they could easily fund a vetting process if they chose.

22. Some employ automated image/text recognition systems that can detect many pieces of illegal content; but these are not totally reliable and, until they are, they must employ human beings as the final safety net.

23. As for who should be responsible for this, the normal laws of the land serve to deter print publishers and this should be true for anything published online. However, a body such as Ofcom may be more appropriate, better resourced and better equipped to apply national legislation.

24. In the UK the Advertising Standards Authority (ASA) regulates all advertising online; companies who flout the ASA Cap codes are censured but the platform that has allowed them to appear is not. The current cases of fraudulent, 'fake'

ads featuring personalities without their consent is instructive. Those ads should never have been accepted. The platform which hosted them talks about being unable to prevent them appearing because the company which placed them is based overseas. Surely, no company which cannot be pursued through the law should be allowed to place any advertising.

What role should users play in establishing and maintaining online community standards for content and behaviour?

25. Users do provide a very helpful detection service, but it is irresponsible to rely on it. This approach also become less and less valuable the more content is personalised through algorithms.

What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

26. The Cambridge Analytica/Facebook scandal brought many of the issues at stake to light. Firstly, the use and abuse of personal data: people should have a right not to be tracked and then, even if they consent to be, not have their personal data shared with any other party without their express, informed consent.
27. Many people have talked about the sinister nature of political ads that are personalised and not openly viewed, where assertions might be made that merit challenge. In truth, the same transparency should apply to any advertising. All brands should be able to know what a competitor might be saying; this is a fundamental aspect of a self-regulatory system.

What information should online platforms provide to users about the use of their personal data?

28. Full disclosure, easily available and easy to understand. No use should be made of the personal data without informed consent and no third party should be given access to it, for free or for money.

In what ways should online platforms be more transparent about their business practices — for example in their use of algorithms?

29. Many users are not aware of how content, including news, is being personalised using their own data, although they are becoming more aware (and resentful) of personalised advertising. It would be easy to have a visible marker on any content to alert the user that what they are seeing is based on personal data, and easy to turn this functionality off.

What is the impact of the dominance of a small number of online platforms in certain online markets?

30. The enormous profits and market share of the leading internet companies is a good indication of how dominant they have been allowed to become. This is

not a situation we would tolerate in any other market, at least, not without paying some sort of monopoly tax. Their dominance is making it very difficult for other media companies which rely on advertising to move their businesses online, whether this be newspapers, magazines, radio or TV services. This is extremely threatening to UK culture and democracy and we welcome the recommendation in the Committee's recent report on 'UK advertising in a digital age' that the Competition and Markets Authority should investigate the online advertising market to ensure it is working fairly for consumers and other businesses and whether current competition law requires change.

What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

31. The European Union has, to date, been the most effective body globally in tackling some harmful internet practices (e.g. protecting personal data privacy via GDPR) and market distortions (e.g. Google anti-trust action). It is to be hoped that the UK will continue to align itself with the EU on these issues, and seek global solutions.

11 May 2018

The *Times*, The *Guardian*, and *Wired UK* – oral evidence (QQ 152-160)

Transcript to be found under The *Guardian*

Mark Bridge, Technology Correspondent, The Times – supplementary written evidence (IRN0118)

What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

The biggest US firms appear to be most concerned about US regulators and the EU. It's illustrative that Facebook's Mark Zuckerberg has appeared in front of politicians in the US and in the European Parliament but has turned down repeated requests to answer questions from the UK's DCMS Committee.

However, the UK has led much of the backlash at these companies' practices and their lobbying budgets in Westminster have increased recently (with Facebook, Google and Amazon employing 50 people to try to influence policy here, according to a recent estimate by the Daily Telegraph).

British newspapers have exposed some of the worst dangerous and harmful content on these sites and our politicians have been among the most outspoken in criticising the companies and highlighting their failings - adding to scrutiny worldwide. We've got some of the world's best academics and artificial-intelligence experts - who can propose solutions - so should work with other governments and regulators to make sure Britain continues to play a central role.

What other international bodies should the UK work through to improve internet regulation?

It should continue to work closely with the European Commission, which has taken a major role in addressing these problems, and with individual governments, such as France, Germany and Spain that are grappling with the same issues and studying or attempting their own remedies. It should also work with the Federal Trade Commission and US government to try to foster a collaborative relationship between lawmakers on both sides of the Atlantic. This is especially important when cultural differences in perceptions of state intervention, and a mistrust in the US of anything that could be seen as heavy-handed, has historically permitted US-based tech firms to have a relatively easy ride on home turf.

12 November 2018

TripAdvisor - written evidence (IRN0106)

General remarks

1. Founded in 2000, TripAdvisor is the world's largest travel website[1190], enabling travellers to plan and book travel and holidays. It offers advice from travellers and a wide variety of travel choices and planning features with seamless links to booking tools for accommodations, restaurants and attractions. Our stated mission is "*to help travellers around the world plan and book the perfect trip.*"

2. TripAdvisor-branded websites make up the largest travel community in the world, reaching 455 million unique monthly visitors, and more than 600 million reviews and opinions covering more than 7.5 million accommodations, restaurants and attractions.[1191] The sites operate in 49 countries worldwide and in 28 languages.

3. TripAdvisor has revolutionised the travel industry. Travellers are no longer limited to opinions and information on limited number of hotels in guidebooks, journalists' articles and properties' own marketing materials but have access to experiences of millions of other consumers, which help them to make more informed decisions. By offering the visibility to the smaller properties with little or no marketing budget, it has also levelled the playing field for hospitality businesses.

4. The best travel advice comes from other travellers. We, therefore, stand for consumers having a voice and the right to share their genuine experiences concerning the places they visit, positive or negative, regardless of where they live, who paid the bill or who disagrees with their opinion. Owners have also a right to directly reply to reviews of their business, which ensures a balanced discussion and provides travellers with better information. Analyses suggest that improved ratings can be directly linked to management responses either to positive reviews or negative reviews.[1192]

5. Transparency is good for consumers and businesses alike and improves service standards. 80% of business owners agree that online review sites like TripAdvisor have a positive impact on hospitality industry and service standards. The confirmation provided by a critical mass of reviews also helps consumers build an accurate picture of a place.
6. TripAdvisor is a website built substantially upon user-generated content ("UGC"). It is free for any business to be listed. The "Traveller Ranking" compares businesses based on traveller reviews of that property as ranked

[1190] Source: comScore Media Metrix for TripAdvisor Sites, worldwide, April 2018

[1191] Source: TripAdvisor log files, Q4 2017

[1192] https://hbr.org/2018/02/study-replying-to-customer-reviews-results-in-better-ratings against other properties in the same city or town, as measured by the quality (number of ‘bubbles’), quantity (number of reviews), and recency of the reviews on TripAdvisor. We offer also the possibility to users to filter the search results with different criteria such as price, distance and availability.

7. TripAdvisor connects users with providers of travel accommodations and travel services around the world, and in doing so, takes significant effort to ensure the reliability of the content found on our website. One primary way we do that is through the establishment and enforcement of a strict firewall between our UGC and our commercial activities, namely online advertising. In order to maintain the trust of our users, advertising payments and the teams associated therewith are completely segregated from our content tools and teams in order to ensure impartiality and consistency in the processing of UGC. Similarly, when an attraction or a restaurant is bookable on one of our subsidiaries and/or TripAdvisor, that fact does not influence its ranking on TripAdvisor or any other aspect of the content made available to travellers. We derive substantially all of our revenue from advertising, primarily through click-based advertising and, to a lesser extent, display-based advertising.

8. No one has greater incentive than us to protect the quality and accuracy of content on our site. If people did not find our information accurate they would not keep using us. That is the reason why since the beginning we have developed an active content moderation and integrity policy. One purpose of that policy is to fight what we call “review fraud” – that is, the submission of suspicious and non-genuine reviews. We are constantly enhancing these systems and our investigations. In doing so, we leverage a combination of best-in-class fraud identification and filtration technology with a team of almost 300 content specialists. These automated systems also serve to screen out unacceptable language, such as swear words and racial slurs.

9. Reviews are not published automatically. All reviews have to go through a strict process successfully before being published. Firstly, every single review goes through our automated tracking system, which maps the how, what, where and when of each review in addition to the language used. If the algorithm detects something in clear breach of our “Guidelines of Publication”, for instance vulgarities, it is not published and the user is informed and asks to write a new review complying with our Guidelines[1193]. If there is some doubt about a review that has been flagged, our content team will assess whether or not to publish the review against our Guidelines.

10. In addition, the team examines every review that has been flagged by a business owner or a user using our dedicated, on-screen reporting tools if they consider that a review breaches our Guidelines and/or infringes their rights. They also conduct proactive investigations to catch would-be fraudsters, using techniques similar to those adopted in the credit card and banking sector. In

[1193] https://www.tripadvisorsupport.com/hc/en-us/articles/200614797-Our-guidelines-for-traveler-reviews

2016 alone, we identified, investigated and shut down more than 60 companies offering to write online reviews for money.

11. This moderation and integrity policy is explained on our website[1194], and TripAdvisor organizes special training events, also together with local trade and hospitality associations – on how to deal with consumers and reviews. The difficulty is sometimes for business owners to tell the difference between "defamatory" reviews and lawful, genuine negative reviews. Whilst our Guidelines and our user terms and conditions[1195] prohibit users from posting defamatory or otherwise unlawful material, we support consumers' rights to share their genuine experiences, whether negative or positive, with each other.

12. As online reviews have a massive impact on the tourism sector in particular, TripAdvisor was also happy to contribute to and to be one of the first signatories of the 'Recommendations on the Responsible Use of Ratings and Reviews on Digital Platforms'[1196] of the United Nation World Tourism Organization. Those best practices provide recommendations for all stakeholders, namely the platforms, the individuals and the businesses. For instance, platforms are advised to put moderation policy in place, individuals to avoid '*personal attacks*' in their reviews and the businesses to '*bear in mind that the large majority of reviews are unproblematic, either positive or negative; both tend to be well-founded*'. Those Recommendations reflect the work on online reviews done by the International Consumer Protection and Enforcement Network under the leadership of the CMA.[1197] The federation of the German consumers' organisations have also recently finalised a study qualifying as 'conscientious' platforms having a three-step-approach to moderate reviews; i.e. an automated review system, plus a team for manual investigations and user-related control mechanism (possibility for users to report reviews).[1198]

Questions:

1. Is there a need to introduce regulation for the internet? Is it desirable or possible?

13. The Internet is very diverse with multiple players relying on different business models. The digital economy is also in constant and rapid evolution. It seems, therefore, difficult to formulate common rules, from which similar obligations will derive without slowing down innovation and new services. For example, what might seem like a reasonable regulation to a massive conglomerate in the online search space could be crippling to a new, innovative search engine

[1194] https://www.tripadvisorsupport.com/hc/en-us/sections/200154967-Fraud
[1195] https://tripadvisor.mediaroom.com/uk-terms-of-use
[1196] http://www2.unwto.org/sites/all/files/wcterecommendationsratingsandreviews.pdf
[1197] https://www.icpen.org/
[1198] https://ssl.marktwaechter.de/sites/default/files/downloads/untersuchungsbericht-bewertungsportale.pdf

that would never be able to get started with massive regulation overhanging it.

14. The digital markets are highly competitive bringing more innovation at better prices to consumers. Compared to the offline market, it is usually easier for new players to start their business and to scale up as the barriers to entry are generally low. Adopting a regulation will stifle the dynamism and the innovation of the digital economy making potentially more difficult for new players to emerge. Regulation would also take years to get adopted and risk to be also outdated at the moment of its entry into force due to the rapid developments of technologies.

15. Furthermore, the existing set of European and national rules regarding fair competition, commercial agreements, privacy and consumer protection, which are also applicable to digital economy, have proved to be able to provide the appropriate regulatory framework to enable the digital economy to flourish. Instead of creating new specific internet rules, enforcing those rules would help businesses to scale up by ensuring fair and competitive market for all players while increasing consumers' satisfaction. Even though online platforms and other digital players have a real impact on the economy it would be counterproductive to create specific rules for them. There are not two opposing economies, offline and online, but rather one economy with two complementary channels, online and offline.

16. As it is currently undertaken by the EU level, there may be some need to review at the margin some existing laws in order to better adapt them to the new digital services and products. It was the case with the General Data Protection Regulation, which was built on the basis of the Data Protection Directive taking over the same legal principles.

2. ***<u>What should be the legal liability of online platforms be for the content they host?</u>***

17. The current intermediary liability regime provided by Articles 14 and 15 of the e-Commerce Directive, implemented in the UK by the Electronic Commerce Regulations 2002, was intended to stimulate investment in an Internet economy that would otherwise be discouraged by overbroad liability, and to provide remedies against unlawful content while facilitating collaboration between online service providers, rights-holders, law enforcement, and other relevant stakeholders. The regime has achieved both of these objectives, establishing a balanced approach to enforcement. In light of the incredible volume of online activity that takes place today, the liability regime helps safeguard and fortify online intermediaries, big and small, old and new. Research has shown that investment in online services would be stunted[1199] if

[1199] Booz & Company, Inc., The Impact of U.S. Internet Copyright Regulations on Early-Stage Investment A Quantitative Study, at 22 (2011), available at online service providers faced strict liability and statutory damages for the misconduct of a minority of its users.

18. As explained above, regarding online reviews, TripAdvisor has taken from its creation a responsible approach to moderate its content. It does not publish reviews automatically. Before being published, all reviews have to go successfully through a strict process, including a combination of (i) best-in-class filtration technology, along with (ii) a team of content specialists, to check if they meet TripAdvisor's Guidelines for publication.[1200] In addition, the team manually examines every review that has been reported by a business owner or a user using the on-screen flagging tool or a web form.

19. However, the Directive only exempts '*information society service providers*' that are merely '*hosting*' content uploaded by users on their website. Judges in a number of EU jurisdictions have determined that platforms like TripAdvisor are '*mere hosts*' even in cases where a moderation policy is in place.[1201] TripAdvisor considers that to be the correct position, as TripAdvisor does not have editorial control over what its third parties' users choose to write and does not amend their reviews once submitted.

20. Nonetheless, there remains real doubt and inconsistency as to whether some courts may erroneously adopt a counter-intuitively and counter-productively strict interpretation of the e-Commerce Directive, such that moderating UGC *at all* risks losing the protections of the e-Commerce Directive. In the case of defamation proceedings, in view of possible legal uncertainties and wrong interpretations of the e-Commerce Directive and of other defamation-related rules, clarification of the liability regime to exempt online platforms who have implemented a moderation process would be therefore highly welcomed. It would avoid the absurd situation where an online platform doing nothing to secure its content would be able to benefit from the non-liability regime, while an online platform taking voluntary, responsible, proactive measures to detect clearly problematic content would be denied the benefit of it. Such a result would result in much more harmful material being posted online, not less. It would also help to prevent the chilling effect on users' freedom of speech that may otherwise result from claimant lawyers making legal threats against responsible, moderating internet platforms to force the removal of lawful, but critical user-generated content. Therefore, to give addition legal certainty to online platforms acting in good faith, a person moderating only offline and online statement (for example, by removing obscene language, correcting typographical errors without altering the substance of the statement or by using automated and/or human processes with a view to accept or reject the

http://www.strategyand.pwc.com/media/uploads/Strategyand-ImpactUS-Internet-Copyright-Regulations-Early-Stage-Investment.pdf

[1200] https://www.tripadvisorsupport.com/hc/en-us/articles/200614797-Our-guidelines-for-traveler-reviews

[1201] Decision of Tribunal de Commerce de Paris in the case *La SARL Hotel Marengo vs TripAdvisor LLC*
Decision of the Court of Imperia (Italy) in *Pascucci vs TripAdvisor LLC*
Decision of the Court of Grosseto (Italy) in *Cala Piccola Spa vs TripAdvisor LLC*

statement) should not be considered as author, editor or publisher. Defamation laws could be reviewed in this respect.

21. This legal change will be aligned with developments at the EU level where the European Commission has developed legal guidance to promote '*voluntary measures'* for online platforms, to secure the integrity of their content while recognizing the non-liability regime under the e-Commerce Directive.[1202] In the Communication, the Commission's conclusions regarding the proactive measures taken by online platforms are as follows:

22. *'The Commission is of the view that proactive measures taken by those online platforms which fall under Article 14 of the E-commerce Directive to detect and remove illegal content which they host – including the use of automatic tools and tools meant to ensure that previously removed content is not re-uploaded –* ***do not in and of themselves lead to a loss of the liability exemption****.*

23. *In particular, the taking of such measures need not imply that the online platform concerned plays an active role which would no longer allow it to benefit from that exemption. Whenever the taking of such measures lead to the online platform obtaining actual knowledge or awareness of illegal activities or illegal information, it needs to act expeditiously to remove or to disable access to the illegal information in question to satisfy the condition for the continued availability of that exemption.*

24. ***Online platforms should do their utmost to proactively detect, identify and remove illegal content online****. The Commission strongly encourages online platforms to use voluntary, proactive measures aimed at the detection and removal of illegal content and to step up cooperation and investment in, and use of, automatic detection technologies.'*

25. The Commission also makes clear that while this legal guidance applies to all categories of illegal content it is important to recognize the fact that different types of content may require different treatment:

26. '***What is illegal is determined by specific legislation at the EU level, as well as by national law****. While, for instance, the nature, characteristics and harm connected to terrorism-related material, illegal hate speech or child sexual abuse material or those related to trafficking in human beings are very different from violations of intellectual property rights, product safety rules, illegal commercial practices online, or online activities of a defamatory nature, all these different types of illegal content fall under the same overarching legal framework set by the E- Commerce Directive. In addition, given the significant*

[1202] The Commission adopted on 28 September 2017 a Communication with guidance on the responsibilities of online service providers in respect of illegal content online and a Recommendation on measures to effectively tackle illegal content online on1 March 2018.

> *similarities in the removal process for these different content types, this Communication covers the whole range of illegal content online, while* ***allowing for sector-specific differences where appropriate and justified.'***

27. In addition, consumer protection laws, such as the Unfair Commercial Practices Directive (UCPD) Guidance published in May 2016, and enforcement bodies, such as the CMA[1203], already raised the importance for online platforms to have policies in place to moderate online reviews. Those 'voluntary measures' to tackle illegal activities and breach of internal guidelines cannot, however, be considered as a general recognition by the platforms concerned to generally monitor their content or to seek facts or circumstances indicating illegal activity.

28. In parallel, the Notice-and-Action mechanism under the e-Commerce Directive efficiently complements the liability protection given to the online service providers. It gives to the online service providers enough flexibility and legal certainty to develop innovative tools and processes to detect illegal content.

29. Considering the above, making online platforms automatically liable for illegal content they host will be detrimental to innovation and will stifle lots of the benefits of the Internet. It will also chill freedom of expression as online platforms may well be placed in a position that, considering the high likely legal risk of being considered liable, they may decide to avoid any risk at all and not publish the content in case of doubt. In order to be on the side of caution, more content than necessary may likely be blocked by the online platforms. After only few months, the implementation of the Germany's Network Enforcement Law, or NetzDG[1204], shows by the example the abuses, the complexity and the ethical questions of a strict liability regime imposed on the online platforms. The German legal requirement that hate speech must be removed within 24 hours leaves platforms very little time to consider questionable content so to avoid any risk and heavy fines (up to €50 millions) platforms opt for the immediate removal of content that appears to fall into proscribed categories of speech.[1205] This overpolicing is exacerbated by the exponential increase in user-generated content being submitted to online platforms.

30. In the case of TripAdvisor, the relevance of our website for consumers and businesses alike would be at stake if negative reviews that could be potentially perceived as defamatory are more systematically not published due to the

[1203] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/436238/Online_reviews_and_endorsements.pdf

[1204] See here below a translation in English the NetzDG: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2

[1205] Facebook has stated that it currently "remove[s] more than 80% of the reported [hate speech] which has been classified as illegal by German non-governmental organizations . . . ." Richard Allan, *We Are Working Hard To Fight Hate Speech and Have Already Made Great Progress*, Facebook (June 19, 2017), high legal risk and possible fines. That would contradict the guidance of the consumer protection enforcement agencies, including the CMA,[1206] calling to treat equally negative and positive reviews. Furthermore, any restrictive law will go against the UCPD guidance providing that '*All reviews, even negative ones, provided they respect legislation against defamation and comply with the terms of service of the site, should be published and should not be pushed at the bottom of reviews to ensure the full and transparent information of consumers.'*

31. **The rule should continue to be that, in case of doubt regarding the defamatory or the illegal nature of a content, the online platform should leave it until a court or an enforcement agency decides on the illegal nature of the content and notifies the platform to remove it. In such cases, only if the online platform fails to remove the notified content, should it be held liable.**

32. **The current liability regime for online platforms, coupled with a notice-and-action process, proves to be both balanced and efficient. Legal guidance on voluntary measures that online platforms could take to tackle illegal content online and securing the non-liability of those online platforms acting in good faith would give the tools and the adequate legal certainty necessary to have more platforms, big and small, acting responsibly.**

3. How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

33. We believe that our moderation and integrity policy explained above is effective. In fact, when we ask our travellers how they found TripAdvisor hotel reviews, 93% say the reviews accurately reflected the trip they took.[1207] Our Guidelines of publication are available online and users are referred to them should a submitted review be in breach thereof. In such a case, the reviewer is informed of the breach and encouraged to submit a revised review that meets the site's Guidelines.

34. Clear information and education tools on the platform to the users help to establish trust into platforms' moderation policy. On TripAdvisor, users can find a guide to write helpful reviews including 10 tips from TripAdvisor reviewers.[1208]

[1206] https://www.icpen.org/

[1207] Source: PhocusWright Customs research, May 2015

[1208] https://www.tripadvisor.com/TripNews-a_ctr.reviewerguideEN

4. What role should users play in establishing and maintaining online community standards for content and behaviour?

35. As is the case on TripAdvisor for online reviews, users (individuals and businesses owners) should have the possibility to flag any problem with a content in order for the online platform to analyse it internally. However, this 'right of flagging' cannot be understood as a 'right of deletion'. The online platform must remain free to keep or take down the content concerned, where the alleged "illegality" of that content is not apparent. In such cases, only a court order or a decision by an enforcement authority should compel the platforms to take down the content.

5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

36. As explained in our response to Question 2, online platforms should put in place appropriate moderation policies, inform users of their moderation and publication policies,[1209] and allow users to flag problems with published UGC.

37. Regarding online reviews specifically, the International Consumer Protection and Enforcement Network under the leadership of the CMA[1210] recommended that '*Review administrators should be guided by the following key principles:*

- *'be equal and fair in the collection of reviews*
- *be alert and proactive in the moderation of reviews*
- *be transparent in the publication of reviews. […]*

Review administrators should remove, or tag as suspicious, reviews where the content is reasonably suspected of being fake, offensive or defamatory. However, review administrators should not:

- *remove genuine reviews solely because a business or individual has lodged a complaint about the review;*
- *approach reviewers with incentives which are tied to the consumer amending or removing a review;*

[1209] See information on TripAdvisor's content integrity and guidelines for traveler reviews

[1210] https://www.icpen.org/

- *apply disproportionately more rigorous checks on negative reviews than positive reviews.'*

38. Following those principles will ensure online platforms using reviews to protect freedom of expression, while acting responsibly to moderate their content, for the benefits of the consumers and businesses alike.

6. ***What information should online platforms provide to users about the use of their personal data?***

39. Data is key for all companies, online and offline, big and small, to run their business. This is true as well for the public sector.

40. For 20 years, the Data Protection Directive has been successful in establishing rules, which have allowed the digital economy to appear and grow while protecting the privacy of individuals. The pragmatic, forward-looking and consistent application of the General Data Protection Regulation in the EU should continue with the new General Data Protection Regulation to defend privacy and allow data driven businesses to thrive.

41. Legal certainty for individuals and business is key to ensure compliance and trust.

42. On one side, users should be informed of their rights regarding their personal data. In particular, they should be certain that their personal data will be protected by the online platforms. The UCPD guidance provides especially that *'the control of reviews should be carried out with respect to users' rights to anonymity in compliance with EU/national data protection laws and should not discourage online engagement or create barriers for consumers to post reviews'.*

43. On the other side, online platforms should continue to be able to collect and process data to offer the best services to their users, including to tackle fraud. For instance, in addition to using advanced content moderation processes, TripAdvisor continuously innovates to develop new products to assist businesses, especially the smallest ones, to get the most out of the rich data generated by TripAdvisor so that they can improve their business and the experience of their customers. Many of those products are available for free.[1211]

44. Furthermore, education is fundamental to help internet users, especially the youngest ones, to protect their privacy.

[1211] https://www.tripadvisor.com/TripAdvisorInsights

7. In what ways should online platforms be more transparent about their business practices – for example in their use of algorithms?

45. TripAdvisor already explains to its users (business partners and individuals) how the "*popularity Index*'[1212] ranks results. It provides the key information to establish trust and, for businesses, we also provide tips to improve their ranking[1213]. There is no need to go beyond this level of information.

46. This current information practice largely applied by online platforms already will actually become a legal obligation once the European Commission's legislative proposal to amend the Consumer Rights Directive (CRD) will be adopted. It provides that online platforms have to inform the consumers about the main parameters determining the ranking of the results. On the side of the businesses similarly, the European Commission's legislative proposal on 'platform-to-business' relations also provides that the platforms shall set out the 'main parameters determining ranking' in their Terms and Conditions. Considering those upcoming legal obligations there is no need to have additional national laws. The worst case scenario would be, like in France, to have national prescriptive and detailed information obligations, including about the display of the website, imposing platforms to come up with country's specific solutions.

8. What is the impact of the dominance of a small number of online platforms in certain online markets?

47. Notwithstanding the growth of TripAdvisor, the markets for travel advertising services and for travel reviews are intensely competitive. We face competition from a number of different offline (e.g., travel agencies, tours operators, newspapers) and online (e.g., search engines, social media sites, online travel agencies, metasearch sites) sources. Many of our competitors have significantly greater and more diversified resources than we do and may be able to leverage other aspects of their business to enable them to compete more effectively against us. As long as this is done in compliance with applicable competition rules, this is positive for consumers and triggers innovation in the business community. However, as for any other sector, competition rules should be enforced in order to quickly cease any abuse of a dominant position by an online platform.

48. The European Commission has found Google being liable to abuse its dominant position as a general search engine provider in the EEA Member States. On the comparison shopping market, Google's preferential display of its own services (Google Shopping) on the top of the general search results page harms competitors and consumers. The more favorable insertion of Google's vertical

[1212] Information on Popularity Index to users here and to businesses here

[1213] TripAdvisor Popularity Ranking Key Factors and How to Improve service compared to the most relevant general search results leads to significant diversion of traffic away from the most relevant results. Google has been asked to provide equal treatment to competitors. The same discriminatory practices are applied on the travel/local vertical search markets. For instance, when consumers run a general search for 'London hotel' on Google they are looking for results that are links to the most relevant vertical search sites (such as TripAdvisor, Expedia or Booking.com) that they can click through to, so that they can run their specialised search using search criteria like stay dates, price range, reviews, star ranking or amenities. Users are not looking for randomly selected hotels (or hotels selected by Google because they pay Google the most). However, today, the consumers see a large box featuring a map and some hotels, which is a Google's product, before the most relevant general search results.

49. Remedies exist to ensure fair competition among online platforms.

50. We are confident that the European Commission, national courts and national competition authorities in the EU and in the UK in particular will continue making decisions in the interest of the consumers and other competitors.

9. What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

51. The BREXIT creates business and legal uncertainties. As stated above, we believe that no specific regulation is necessary to regulate online platforms or Internet. As any other business activities, online platforms are already regulated by existing applicable laws, European and/or national, including the e-commerce and services Directives, competition and consumer protection rules. Instead, providing guidance, if necessary, would ensure compliance with applicable laws and underscore trust for consumers and business alike. Such guidance would also prevent the adoption of conflicting rules between the UK and the EU.

52. It would be essential for the UK to avoid conflicting rules with the EU preventing or creating red tape for companies to do business. For instance, having clear rules for data transfer between UK and EU is pivotal.

53. Company and industry best practices could complement the set of existing rules to enhance compliance and trust and allow the flexibility to cope with innovations.

June 2018

Twitter and Match Group – oral evidence (QQ 122-127)

Transcript to be found under Match Group

UK Computing Research Committee (UKCRC) – written evidence (IRN0011)

> The UK CRC is an Expert Panel of all three UK Professional Bodies in Computing: the British Computer Society (BCS), the Institution of Engineering and Technology (IET), and the Council of Professors and Heads of Computing (CPHC). It was formed in November 2000 as a policy committee for computing research in the UK. Members of UKCRC are leading researchers who each have an established international reputation in computing. Our response thus covers UK research in computing, which is internationally strong and vigorous, and a major national asset. This response has been prepared after a widespread consultation amongst the membership of UKCRC and, as such, is an independent response on behalf of UKCRC and does not necessarily reflect the official opinion or position of the BCS or the IET.

Response to Questions

1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

[Paragraph 1] We would like to clarify confusion in the use of the term Internet; which refers both to the technical infrastructure - concerned with addressing hierarchies, routing policies, domain naming service, and other elements of the communications infrastructure – and the content and higher-level (web) applications delivered over that infrastructure. Attempts to regulate the latter are constrained by the open policies that dominate the former. For example, placing restrictions on Internet applications in the UK may only encourage people to manipulate the internal mechanisms to hide their location or to access those applications within the UK in ways that cannot easily be monitored or detected. We would encourage subsequent enquiries to honour this distinction in the usage of the term in such a vital area for the future of our connected nation.

[Paragraph 2] With this distinction between Internet infrastructures and Internet applications in mind, and in response to question 1, we note two different responses in different areas of industry. Large US Web application service providers (Google, Facebook, Amazon, Twitter, etc.) tend to argue in favour of the status quo; supporting 'net neutrality'. In contrast, the large telecom providers tend to argue in favour of regulation. This is not antithetical. Regulation may be necessary at the application level to ensure social goods: privacy, free speech etc., while Net neutrality sustains the Internet "pipes" and end-to-end communication service. In technical terms, we see a regulatory divide at the boundary between end-to-end Internet connectivity (in more technical terms the equivalent of the OSI Transport Layer) and the content and higher-level (e.g., web) applications

[Paragraph 3] The greatest danger is that the conflation of these different usages of the term 'Internet' create a regulatory environment in which it is possible for businesses to "own" vertical slices that control both application level services and the underlying communications infrastructures to the possible detriment of their competitors.

2. What should the legal liability of online platforms be for the content that they host?

[Paragraph 4] Such a question cannot be answered except in terms of high-level principles that must be interpreted by a court of law or by devolving responsibility through a regulatory body/ombudsman similar to the Independent Supervisory Authority described in the General Data Protection Regulation (GDPR). The dynamic nature of Internet services makes it very difficult to draft detailed definitions of legal liability in this area. This creates concerns that law may be misapplied in a context that was never intended by those developing the original legislation.

[Paragraph 5] The existing organisations lack the resources to support the implementation of even existing legislation in any but the most extreme cases. Evidence for this can be provided through a research project led by our members[1214]. The fast-changing nature of Internet communication and the number of people accessing shared resources around the globe undermine attempts by police, councils, news agencies, anti-harassment organisations, anti-bullying groups and schools to combat inflammatory, antagonistic or provocative material. *Any regulatory agency must be adequately resourced to address existing public concerns and support those agencies already struggling to respond to complaints about Internet content.*

3. How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

[Paragraph 6] Existing platforms provide few or no guarantees over moderation. Most rely on self-moderation with explicit procedures only being activated after complaints are received. We also recognise widespread dissatisfaction at the result of requests for intervention. However, we recognise that this area is changing; for example, as a result of Mr Justice Warby's ruling in the High Court over the 'right to be forgotten' and as a result of GDPR (Article 16 on the right to rectification, Article 17 on the right to be forgotten).

[Paragraph 7] We recommend a code of practice that explicitly promotes transparency in moderation and provides a reference point for best practice. We do not advocate legislation for the reasons mentioned previously (see paragraph 4).

[1214] The ESRC Digital Wildfire project[1214] was an interdisciplinary collaboration between the Universities of Oxford, Warwick, Cardiff and De Montfort, see http://www.digitalwildfire.org/

4. What role should users play in establishing and maintaining online community standards for content and behaviour?

[Paragraph 8] On-line communities play a strong role in maintaining standards and this should be recognised. However, we cannot rely on them. These communities often reflect the particular interests of a subset of users. They often do not reflect the norms and values of society as a whole. There are tensions between the necessity to support free speech, the corrosive impact of perceived censorship and the need to safeguard expectations of public behaviour. A regulatory organisation, armed with a code of conduct, could mirror some aspects of the National Cyber Security Centre’s work in educating on-line communities and providing case studies of the negative consequences of failing to act before an incident takes place.

5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

[Paragraph 9] This has been addressed in previous paragraphs. However, a transparent approach to moderation should be adopted – in line with a proposed code of conduct. We would also recommend that such policies by proportionate to the changing audiences – for example, the operators of online platforms should employ more active moderation in applications that attract a school-aged audience.

6. What information should online platforms provide to users about the use of their personal data?

[Paragraph 10] This is largely covered by GDPR but the public understanding of this directive remains very poor. As mentioned in paragraph 8, we welcome a strengthened regulatory organisation with responsibility for informing the public about their rights in this respect and also to ensure companies meet public expectations. This is an imperative if we are to go beyond the present difficult situation in which it takes a major breach of trust before many users realise the possible applications for the data they provided in response to on-line quizzes etc.

7. In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

[Paragraph 11] Programmers often like to think that the algorithms they develop are “neutral”. In practice they can create biases – e.g. in page ranks or what kinds of posts dominate social media streams. These influences are often subtle and unintended. There is a need for basic research to develop metrics and methods to discover these biases so that we can make developers more aware of the potential dangers. Similar comments can also be made about companies that deliberately seek to exploit these biases; as recent events have shown.

[Paragraph 12] There is a natural reluctance for companies to disclose IPR – it is important that UK legislation does not stifle innovation in the provision of data services that have the prospect of offering significant prosperity and public good. There is also a concern that the UK should not develop legislation that can simply be avoided by technical innovation in the underpinnings of the Internet – for instance through moving servers to other jurisdictions. Equally, for responsible operators, the proposed code of conduct could be associated with a traffic light system or some other suitable visualisation to help members of the public identify the degree of protection and moderations supported by a particular platform.   We do not wish online platforms to divulge implementation details or innovative aspects of the algorithms they use. They ought to be more receptive to criticisms about any bias or dominance that the algorithms are observed to introduce into their results – and that an appropriate regulator might have the power to go and negotiate if and when users or relevant bodies complain.

8. What is the impact of the dominance of a small number of online platforms in certain online markets?

[Paragraph 13] This call is timely – it comes at a moment of significant change in the public perception of these dominant on-line service providers.   It remains to be seen how they will respond.   There is a concern, noted in paragraph 11, that some of these providers are responding by limiting third party access to all of their data – even when it is anonymous and appropriately aggregated. We should not underestimate the negative impact of these restrictions when, for instance, researchers are developing ways to speed the response and increasing information available during emergencies using the information provided by the public through social media. There is a need for more and better informed public discourse about the risks and benefits of data sharing – for what purposes and with what level of guarantees of anonymity.

9. What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

[Paragraph 14] This depends on the extent to which courts recognise each other's jurisdiction and to which UK legislation diverges from that across Europe. This submission has focussed on 'soft measures' – on a code of practiced and on informing companies and the public of expectations of behaviour. More stringent enforcement may be futile because of the dichotomy noted in paragraph 1: the application layer, which is the focus of public concern, is supported by technical infrastructures that do not obey geographical borders or legal jurisdictions. The costs of enforcement are likely, in such cases, to outweigh the public good.

4 May 2018

UK Council for Child Internet Safety's Evidence Group – written evidence (IRN0079)

I write on behalf of the UK Council for Child Internet Safety's Evidence Group to draw your attention to the recent literature review we produced for DCMS in 2017. This reviewed the available recent evidence on how young people are using the internet in the UK, the opportunities and risks associated with this, and the regulatory and safety issues that arise. Our key findings were that:

- Between one in ten children to one in five young teens say they encountered something worrying or nasty online in the past year.

- Few children say they send photos to online contacts or reveal personal information, but a substantial minority use services 'under age'.

- While many UK children have learned to be cautious online, there is little evidence that their digital skills are increasing with time.

- Cyberbullying estimates range between 6-25%+ depending on measures, and the reasons for victimisation are diverse.

- Children's (and parents') top online worries are pornography and violence, often encountered on video sharing sites.

- Children's age and gender, digital literacy and resilience all affect their online experiences and wellbeing outcomes.

We believe it is important that the UK's regulatory environment guides industry, schools and parents so as to be responsive to children's diverse needs and rights, empowering them as well as protecting them in the digital environment. Such guidance should be informed by robust and specific evidence of which risks lead to harm, for whom and under which circumstances, as well as of which interventions work best.

Our evidence review is available at:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650933/Literature_Review_Final_October_2017.pdf and
http://eprints.lse.ac.uk/84956/

The work of the UKCCIS Evidence Group is available at:
https://www.saferinternet.org.uk/research

11 May 2018

UK Music – written evidence (IRN0040)

1. UK Music is the umbrella body representing the collective interests of the UK's commercial music industry, from songwriters and composers to artists and musicians, studio producers, music managers, music publishers, major and independent record labels, music licensing companies and the live music sector.

2. UK Music exists to represent the UK's commercial music sector, to drive economic growth and promote the benefits of music to British society. A full list of UK Music members can be found in annex.

Overview.

3. UK Music's 2017 Measuring Music report UK music industry contributed £4.4 billion to the economy in 2016 - year on year growth of 6%. The UK music industry generated export revenues of £2.5 billion in 2016 - year on year growth of 13% and the UK music industry employed over 142,000 people in 2016.

4. Music is a digital business. In the UK there was a 9.5% increase in music consumption across all formats in 2017. Streaming now accounts for over half of UK music consumption. The success of services such as Apple Music, Spotify and Deezer has meant that last year 68.1 billion audio streams were served in the UK alone.50% of the industry's global revenues now come from digital. The UK is second to the US in terms of the number of licensed music services.

5. The challenge all national governments face is how to encourage innovation and the creation of value without trampling all over legitimate individual and commercial rights and interests or subverting fundamental societal norms. Many of our key arguments are echoed in other debates concerning the internet - whether it be privacy, data protection or harm from unfiltered content. It is also worth noting that the claim that lies beneath the notion of intellectual property is similar to the one that underpins the notion of privacy, having been created by an individual's relationship with the world and concerning how the author retains control over it. Privacy and intellectual property cannot be treated in isolation of one another.

6. In pursuit of innovation and economic growth protections for innovators in the digital space, the net result has not been a sensible equilibrium in which the tech sector has risen in a symbiotic way or been subject to sufficient checks and balances. Conversely it has lead to the creation of some of the biggest companies in the world, often able to defy attempts at

governmental control and steps to level the playing field. There is an urgent need to re-establish the balance between power and responsibility online.

Background.

7. Digital technologies and the online market have changed the way in which music is used and consumed dramatically over the last two decades, providing significant challenges and opportunities for the music industry. This first manifested itself in the late 1990s with the development of peer-to-peer file sharing platforms; services such as Napster and latterly Pirate Bay. The prevalence of pirated music throughout the 2000s impacted on the music industry considerably. 2001 saw the launch of the iTunes store and the first iPod and with it digital downloads, offering legitmate access to digital music. Despite this, online piracy continued to grow throughout the first decade of 21st century. As a result the value of the music industry fell year on year. Not only did the industry face falling incomes but was forced to spend millions enforcing our rights.

8. There are gains as a result of the industry's efforts and investment. For example, networks are being policed that have not had obligations or incentives to act. There has been a gradual decrease in music piracy in the last few years, with the average number of monthly infringing tracks consumed across the four main types of piracy platforms in the UK (bittorrent, stream rippers, cyberlockers & mp3 download) having fallen to 36 million in 2017 from 54 million in 2016, a reduction of 33%. We have also seen an increase in legal consumption during this period. This is not to say that the costs and losses due to piracy to music businesses have not been significant. Platforms have still been able to grow rapidly without regulation and low obligations placed on them.

9. Although traffic has decreased over the past 12 months across the main types of pirate sites, consumers wishing to access music illegally can still do so. Stream ripping sites/apps (which are still operational) allow the consumer access to any music across YouTube and social media, including Instagram, which has recently become popular for discovering new music. Bittorrent & cyberlockers still facilitate large volume piracy – such as back catalogues or recent albums. All popular artists' repertoire is available on these sites. UK Music member the BPI estimates 426 million tracks were consumed from infringing sources in 2017 and that music piracy in the UK costs the music industry over £120 million a year.

10. The code of practice on search engines[1215], agreed last year and facilitated by the Government, shows that there is more that intermediaries can do when challenged. Greater obligations to act are needed for co-operation to

[1215] https://www.gov.uk/government/news/search-engines-and-creative-industries-sign-anti-piracy-agreement

be meaningful. Administrative site blocking and notice and stay down would both reduce music industry costs and make it harder for illegal operations to build and thrive.

11. The music industry in 2018 is a market dominated by digital steaming services rather than downloads and yet the problems of piracy persist albeit in new forms. In addition, the growth of streaming brought with it services which hosted works uploaded by users, most notably YouTube but increasingly social media platforms such as Facebook. These services were able to build global billion dollar businesses based upon advertising while claiming that were not required to seek the authorisation of the rightholders whose works they were making available. The dismantling of the link between the use of music and the need to obtain authorisation from creators, performers and producers has built a transfer of value from the music industry to online platforms.

The problem.

12. This gap between the value realised in the online market and that which is returned to the music industry, is due to a legal framework which is not fit for purpose or relevant to the digital landscape. The current framework permits is some platforms hosting and making available musical works uploaded by their users to avoid obtaining a licence, or in some cases pay significantly less than the market rate for the music they use.

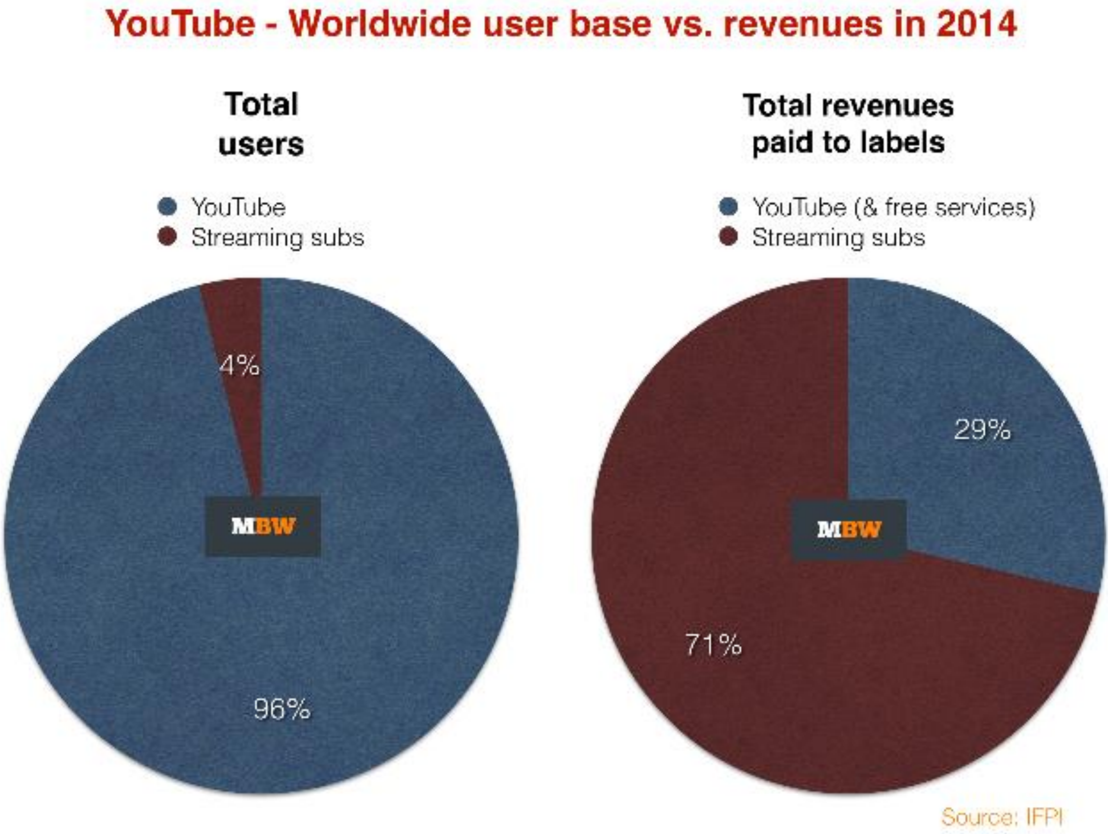
13. Limitations from liability for Internet service providers (so called "safe harbours") provide for across the EU in the e-Commerce Directive 2000) and the United States by Digital Millennium Copyright Act 1998. The limitations in the e-Commerce Directive restrict the liability of information society intermediaries if their activities qualify as mere conduit, caching, or hosting. Notably, these limitations were devised in the late 1990s to help the development of the then nascent digital communications market. In 2018, the digital communications market is well labelled established. Digital communication providers, established considerable time after the coming into force of the e-Commerce Directive and the Digital Millennium Copyright Act, are the main source of access to music and other creative content benefiting from enormous increases in broadband availability and speed.

14. The world has changed. In the late 1990s information society intermediaries were predominantly enabling the sending of digital material such as emailing. The biggest intermediary was AOL providing a dial-up service, a web portal, an email and messaging service as well as an internet browser called Netscape. In 2018 information society intermediaries are the main sources of creative content online; all of these US tech giants were created considerable time after the legislation limiting the liability of information society intermediaries (Facebook: 2004; YouTube (2005 and sold to Google in 2006). These services were clearly not the intended beneficiaries of the limitations of liability in the e-Commerce Directive and the Digital Millennium Copyright Act. Nevertheless, such services often rely on

limitations of liability to reduce the licensing fee for the use of music in negotiations with rightholders or even avoid obtaining a licence altogether.

15. This deprives composers, performers, music publishers and record companies from the remuneration they should be due in a functioning market for their creative endeavours. It also disrupts the legitimate market for online digital music services given that some platforms pay less if anything for music relying on limitations of liability whilst other services de facto offer the same product (i.e. access to music online) and pay the fair amount. The resulting value gap between digital music platforms and online music providers impacts both creators/ performers and legitimate online music providers.

16. The 2014 figures below exemplify that 4% of the users of online music services are responsible for 71% of revenues paid to labels (this has not changed in 2018).



Approach.

I. Clarification of liability of information society intermediaries

17. Liability of information society intermediaries is in urgent need of clarification, at national, regional and international level (given the global

nature of the Internet) in particular as regards online platforms providing access to user uploaded music.

18. UK cases provide such clarity recognising that both the platform and the users of the platform communicate to the public (E.g. Dramatico Entertainment Ltd and others v British Sky Broadcasting Ltd and others [2012] EWHC 268 (Ch), 20 February 2012 Paras 71 and 81 respectively). There is recognition that online platforms providing access to user uploaded music (or other creative works) are communicating to the public by making material available on the platforms; they are also reproducing material on their servers. In as far as they communicate to the public they cannot benefit from any limitation of liability be3cause they are not hosting.

19. Users uploading music to such platforms are also communicating to the public and making reproductions given the technical process involved in their individual computers. Only as regards such activities of users digital platforms might be able to benefit from limitations of liability provided they fulfil the respective qualifications.

20. The currently discussed European Directive Copyright in the Digital Single Market provides a good opportunity to clarify the liability of information society intermediaries de lege lata (in particular Article 13 thereof). Should an effective solution not be adopted at European Union level the withdrawal from the European Union presents a good opportunity for the United Kingdom to develop a clear framework for a fair value chain involving composers, performers and rightholders as well as platforms and digital music providers. The Digital Charter might provide the appropriate vehicle for such activities at national level, be it by legislation or by providing guidance.

II. Stay down

21. Specifically, this should also include an obligation to keep musical works and sound recordings off the platform once notified about their illegitimacy. Currently, rightholders identify illegitimate material made available on digital platforms and notify them about this material. Ideally, digital platforms take this material down following such notices. However, despite effectual content recognition technologies readily available (the competitive market for such technologies includes for instance Content ID; Audible Magic; Gracenote, Shazam etc) the takedown of material is often limited to the actual internet link and not to the actual work thus enabling an immediate re-upload. It is key that digital platforms apply such technologies in order to ensure that the material remains removed from their services. UK Music member the BPI has removed over 605 million links to infringing content across Google and Bing since it began its delisting strategy in 2011.

III. Trade agreements following the withdrawal from the European Union

22. Given our concerns regarding the appropriateness and effectiveness of limitations of liability under both European Union and United States laws UK government needs to assess critically any reference to such systems in future trade agreements with the European Union, the United States, or any other country. If for instance the United States insists on applying their system of limitations of liability for services as they have done in the trade agreement with South Korea this would undermine the UK music industry, a net exporter of music globally, considerably.

Further issues

Secondary ticketing market

23. Reselling at profit in the online secondary ticketing market is a matter of concern. This was highlighted in the recent UK Live Music Census[1216].

24. As a result of the Competition and Markets Authority inquiry three of the four principal secondary ticketing platforms are being forced to obey the law. This is welcome yet the fourth, Viagogo, still refuses to comply and is now under threat of legal action.[1217]

25. Secondary ticketing websites benefit from appearing high in search rankings, often at the expense of primary sources. Google has unveiled new rules regarding ticket resale websites to make it clear they are secondary sites yet Viagogo still appears at the top of online search despite not fully complying with the law.

26. UK Music recommends that the changes made by Google be reviewed three months' after implementation to see if they have proved effective and have prevented the public from being misled.

Limitations of liability of information society intermediaries (e-Commerce Directive)

Mere conduit: Article 12 e-Commerce Directive exempts from liability information society intermediaries who store transmitted information automatically and transiently. This means that in order to qualify for this limitation, the information society intermediaries must not (1) initiate the transmission, (2) select the receiver of information or the actual information contained in the transmission, or (3) modify it. The information transmitted must take place for the sole purpose of carrying out the transmission only, and not be stored for a period longer than reasonable necessary for the purposes of the transmission.

[1216] http://uklivemusiccensus.org/

[1217] https://www.gov.uk/government/news/secondary-ticketing-sites-pledge-overhaul

Caching: Article 13 e-Commerce Directive exempts from liability information society intermediaries which store transmitted information automatically and temporarily "for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request."

Hosting: Article 14 e-Commerce Directive exempts from liability information society intermediaries which store data which are specifically selected and uploaded by a user of the service, and intended to be stored ("hosted") for an unlimited amount of time. Hosting providers can only benefit from the liability exemption when they are *"not aware of facts or circumstances from which the illegal activity or information is apparent"* (when it concerns civil claims for damages) or they *"do not have actual knowledge of illegal activity or information."*

Additionally, the e-Commerce Directive provides that there is no obligation to monitor, Article 15. However in case law the concept of duty of care was developed. The duty of care which information society intermediaries owe to monitor and remove copyright infringing content has not been stated in the legislation. Moreover, Article 15 e-Commerce Directive provides that there is no general obligation on information society intermediaries to monitor. There is hence no general obligation actively to monitor information which is transmitted or stored, or actively seek facts or circumstances which indicate infringing activity. The Court of Justice of the European Union established some parameters of the duty of care owed by information society intermediaries to monitor content. In L'Oreal and others v eBay and others. the Court denoted that the Internet service provider needs to undertake further activities if he has been playing a more "active role "in the infringement in order to qualify for the limitation of liability under the e-Commerce Directive. In the SABAM cases (e.g. SABAM v Netlog), the Court stated that an information society intermediary cannot be obliged to install a general filtering system, covering all its users, in order to prevent the unlawful use of musical works, as well as paying for it. (c.f. Article 15 e-Commerce Directive). The cases were based on the specific facts at hand without providing a specific definition of duty of care.

Limitation of liabilities (Digital Millennium Copyright Act, S 512)
The Digital Millennium Copyright Act limits the liability of online service providers in certain circumstances.

- Transitory communications; (c.f mere conduit);
- System caching;
- Storage of information on systems or networks at direction of users; (c.f. Hosting - knowledge); - Information location tools (not currently included under mandatory European Union provisions, see Article 21 (2) e-Commerce Directive

Annex

UK Music's membership comprises of:-

- AIM – The Association of Independent Music – the trade body for the independent music community, representing over 850 small and medium sized independent record labels and associated music businesses.

- BASCA exists to celebrate, support and protect the professional interests of all writers of music.

- BPI - the trade body of the recorded music industry representing 3 major record labels and over 300 independent record labels.

- FAC – The Featured Artists Coalition represents and promotes the interests of featured recording artists in the music industry.

- MMF – Music Managers Forum - representing over 500 UK managers of artists, songwriters and producers across the music industry with global businesses.

- MPG - Music Producers Guild - representing and promoting the interests of all those involved in the production of recorded music – including producers, engineers, mixers, re-mixers, programmers and mastering engineers.

- MPA - Music Publishers Association - with 260 major and independent music publishers in membership, representing close to 4,000 catalogues across all genres of music.

- Musicians' Union representing 30,000 musicians.

- PPL is the music licensing company which works on behalf of over 90,000 record companies and performers to license recorded music played in public (at pubs, nightclubs, restaurants, shops, offices and many other business types) and broadcast (TV and radio) in the UK.

- *PRS for Music* is responsible for the collective licensing of rights in the musical works of 114,000 composers, songwriters and publishers and an international repertoire of 10 million songs.

- UK Live Music Group, representing the main trade associations and representative bodies of the live music sector.

May 2018

UK Safer Internet Centre (UKSIC) – written evidence (IRN0061)

About the UK Safer Internet Centre:

The UK Safer Internet Centre is a coalition of three charities; The Internet Watch Foundation, South West Grid for Learning and Childnet International with one mission to promote the safe and responsible use of technology for young people. The partnership was appointed by the European Commission as the Safer Internet Centre for the UK in January 2011 and is one of 31 Safer Internet Centres in the INSAFE network. The UK Safer Internet Centre has three main functions:

1. Awareness Centre: To provide advice and support to children and young people, parents and carers, schools and the child workforce and to co-ordinate safer internet day across the UK.

2. Helpline: to provide support to professionals working with children and young people with online safety issues

3. Hotline: An anonymous and safe place to report and remove child sexual abuse imagery and videos, where ever they are found anywhere in the world.

1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

1.1 The UK Safer Internet Centre believes that this question about internet regulation is in essence too broad to answer as one question. To determine if there is a need for regulation, we believe that it should be for politicians and Government to determine what the problem they are trying to solve is. We believe that the requirement for regulation depends on the type of content you are asking industry to deal with and that there might be a mix of regulatory responses.

1.2 For some forms of content, self-regulation is working. Take for example the IWF's model for dealing with the spread of Child Sexual Abuse online. When it was established in 1996, 18% of the world's CSAM was hosted in the UK, today that figure remains below 1%. This is due to their collaborative and partnership approach with the internet industry, law enforcement and Government and being a trusted and authoritative voice on their subject matter.

1.3 One of the challenges with internet regulation is that there is not necessarily broad consensus internationally about what is and isn't illegal, this is particularly an issue for hate speech, terrorist content and other forms of harmful content online, which means that global internet companies are having to comply with many different laws in different jurisdictions over what is and isn't illegal. Ultimately, for the big American companies, they are governed by U.S. law, which means that any investigative process is undertaken by American law enforcement and any illegal content hosted on a U.S. company's platform has to be reported to the authorities by law. Any introduction of regulation or mandatory reporting in the UK, means that it could potentially prejudice law enforcement investigations in the U.S. or duplicate the process.

1.4 SWGfL is responsible for operating the Revenge Porn Helpline (on behalf of the Government Equalities Office) and have just developed a new project to enable the removal of harmful content online. The national reporting hub will provide evidence and step by step guidance on how to report different types of harmful online content, and where appropriate will provide some mediation with social media providers to ensure swift takedown of content which breaches their terms and conditions. It is available to all children and adults in the UK, and will act as a one stop shop for reporting abusive content. It is a strong example of a voluntary initiative between industry and charitable organisations working collectively to help make the UK the safest place to access the internet in the world.

1.5 Currently there are very few good ideas of how to effectively regulate the internet, without damaging the delicate internet infrastructure and eco-system that has made the internet such a valuable asset in the first place.

2. What should the legal liability of online platforms be for the content that they host?

2.1 The e-commerce directive is an exceptionally important part of EU legislation which ensures that companies are liable for the content that they host on their platforms. This legislation is essential to ensuring that enforcement organisations such as the police and the IWF can get the internet industry to take down illegal content online, through notice and take down procedures.

2.2 Similarly, to question one, where there is clear legislation about what is and isn't illegal, it is easier for companies to respond to what should be removed. In the field of Child Sexual Abuse material, the legislation is clearly defined by the Children's Act (1978) and the IWF's operations linked to the Sexual Offences Act (2003). IWF analysts assess in line with UK law, which is set out in the Sentencing Council Guidelines (2014) and is also the same standard used by UK Law Enforcement and in Sentencing by the judiciary.

2.3 Where there is clearly defined legal standards of what is and isn’t illegal, companies are covered by the current liability regime contained within the e-commerce directive, which is a workable solution which currently falls short of statutory regulation. It is clear that there are successes in the current legal regime, but that does not mean that Government, policy makers and legislators should not be constantly looking for ways to improve legislation.

3. How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

3.1 We believe that there is clearly room for improvement in terms of effective, fair and transparency of online platforms in terms of moderating the content that they host. It is fair to say that companies and the debate around illegal and harmful content has come a long way since the inception of the internet in the late 1990s. Many are now willing to discuss the challenges they face in moderating this content than denying its very existence. Google have recently finalised and published its transparency report and Facebook has also announced that it is employing another 10,000 internet content moderators to deal with complaints about content online.

3.2 The UK Safer Internet Centre, however, believes that there needs to be much more investment in research in obtaining feedback from internet users to improve the process for moderating content. Childnet International’s Project DeShame report which interviewed over 3,000 children (ages 13-17) about their experiences of sexual harassment online and found that 43% of respondents didn’t want to report to social media because they believed that it would not help. Companies need to acknowledge when a complaint is made in a timely fashion and then inform users about what action has or hasn’t been taken and why in order to improve confidence in reporting, particularly amongst children and young people.

3.3 The UK Safer Internet Centre Helpline has become a world leader in collaborating with providers and through a deep understanding of their terms and conditions, excelled at taking down harmful content, with 95% of its cases escalated to industry being resolved satisfactorily with the removal of content. Building on the success of this, the Revenge Porn Helpline (funded by the Government Equalities Office) that was launched in 2015 to tackle image based abuse of adults. It has also since supported the Australian eSafety Commissioners Office in establishing their image based abuse Helpline as well as ICanHelp Line in the US.

3.4 It is important that this service is made available to all Internet users, not just children and the UK Safer Internet Centre has the necessary skills and capabilities and experiences to play a significant role in this type of service.

The Harmful Content project will tackle issues affecting the whole internet population specifically Online Abuse, Bullying or Harassment, Threats, Impersonation, Unwanted sexual advances (not image based), violent content, self-harm or suicide content and pornographic content. As part of this work the UK Safer Internet Centre will continue to provide critical advice feedback to platforms on their policies, reporting systems and will assist in improving their platforms for users wherever possible.

3.5 In terms of who could be responsible for overseeing platforms performance of being fair, transparent and effective there are a number of potential models which could be pursued. The Government's Internet Safety Strategy sets out what is expected of Social Media Companies as a result of implementing a new Code of Practice, which establishes what information companies need to be more transparent about which is a useful starting position. The view of the UKSIC however, is that any oversight function needs to be both trusted and independent of both Government and industry. It needs to be independent of Government in order to be free of political interference and in order for companies not to be acting under the instruction of Government and equally needs to be independent of the companies themselves who are by and large driven by commercial activities first and foremost.

3.6 In Australia, an e-safety Commissioner has been appointed, which is responsible for promoting the online safety of all Australians. The Office leads the online safety efforts of Government, Industry and not-for-profit community, with a broad remit which includes a complaints service for young Australians who experience serious cyber-bullying, identifying and removing illegal content and tackling image based abuse.

3.7 The Office of the e-safety commissioner also provides educational resources, e-safety information and wellbeing support and advice. The Commissioner's office also provides research and legislative information about what is and isn't illegal.

3.8 What is clear is that anybody that is responsible for ensuring the criteria set-out in this question needs to be independent, transparent accountability and well-funded in order to deal with some of the inevitable legal challenges it will face, particularly in terms of more questionable decisions to remove content online.

4. What role should users play in establishing and maintaining online community standards for content and behaviour?

4.1 There are a wealth of resources on the UK Safer Internet Centre webpage which provides advice and support to children, their parents and those professionals working with children and young people.

4.2 For children there are interactive games and quizzes, films and advice about staying safe online, with latest blog postings giving advice on how to spot advertising on Instagram and how to control your privacy settings on the platform.

4.3 For Parents, there is advice about safety tools on social media networks and other platforms, a parent's guide to technology, how to have a conversation with your child about safe internet usage.

4.4 The website also provides Teachers with teaching resources, curriculum planning and appropriate filtering and monitoring.

4.5 All three charities that make up UKSIC believe that users play and important part in maintaining standards of behaviour online and that is why we run the UK's Safer Internet Day to encourage greater responsibility of children, parents and carers and those working with children and young people.

4.6 The day has been running in the UK for the last past eight years and the 2018 theme was specifically focussed on promoting more respectful behaviour online with the slogan: "Create, Connect and Share Respect a better internet starts with you." This day reached 45% of children aged 8-17 in the UK and 30% of parents and was supported by over 1700 organisations.

4.7 The UKSIC also believes that there is a need to educate children about the nature of the online world, and clearly there is a role for peer to peer education as our research consistently shows that children are likely to have conversations with each other about their online safety and there is a need for this to be well informed. Childnet's Digital Leaders programme directly empowers children to harness their passion and knowledge of internet safety to become role models for their peers and younger generations so that children know where they can report their differing concerns. Our Need Help? page directs users about where they can report their concerns. Despite all of this information, we believe that there is a need for people to be encouraged to report by platforms and that the process must be easy to use, accessible and with clear processes that are transparent with a tangible outcome, whether positive or negative to the user that is well explained, to encourage them to take responsibility for their online community.

5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

5.1 This submission already mentions a number of safety initiatives adopted by industry in the offline world which practicably assist children and young people in their online world. Safer Internet Day, Childnet Digital Leaders programme and talking to children and young people about their experiences online and helping that to inform policy and future direction of freedom of expression and the protection of rights online is really important work that should be continued into the future. There is currently a lot of discussion within the United Nations about the concept of empowering children as Human Rights Defenders and them becoming much more actively involved in promoting their rights to expression on lots of these issues, something which the UKSIC clearly supports and merits further development and discussion.

5.2 Relating to the online world, we believe there is potentially more platforms can do to offer in app online safety advice and support to children and young people in particular. It would be particularly helpful for platforms to sign post to help and support about making reports of content that users feel shouldn't be online, as well as support on advice about controlling privacy settings as mentioned in previous answers.

6. What information should online platforms provide to users about the use of their personal data?

6.1 The UKSIC believes that there should be clear expectations by online platforms about what personal data they are collecting and what purposes this data is being used for. Terms and conditions need to be much shorter, simpler to understand and should be easily interpretable by children and young people and those groups of adults that are particularly vulnerable due to them having a lower-level of digital literacy or have disabilities for example.

6.2 UK Safer Internet Centre is actively calling for terms and conditions labelling; labelling akin to nutritional labelling displayed on food packaging and laundry labels to inform users as to key components of a product. A mechanism that is helpful and informative to users to visually appreciate key components of the terms and conditions, aspects of the service as well as the acquisition and use of personal data. Clearly data is the 21st Century commodity and has significant and underappreciated value, but 'if data is the currency, then trust is the exchange rate' and this type of labelling, together with the UK Safer Internet Centre reporting channels will help to instil user trust.

6.3 We believe that there should be high levels of control for users as a default, allowing users to choose less privacy settings if they wish. However, as each social media platform is subtly different in reality, this maybe a technical solution that maybe difficult to achieve for some depending on how their platforms are designed and configured.

7. In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

7.1 How public companies should be about the algorithms they use is a complex question as it goes to the heart of the business model on which the internet is built. Algorithms are what gives some internet companies a technical advantage over a competitor and commercial sensitivities do need to be considered, in any demands for greater transparency that balances the need for transparency against the wealth creating benefits of the internet industry.

7.2 Algorithms are also used positively by companies to identify harmful and illegal content online, however, they aren't perfect and we believe that it is important to ensure that in cases where questionable content is identified artificially that a human has the final say in a decision making process to ensure that a high-quality standard is maintained and that contentis not being removed which is legal.

8. What is the impact of the dominance of a small number of online platforms in certain online markets?

N/A

9. What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

9.1 It is difficult to assess the immediate impact of the UK leaving the European Union as it depends on the nature of the deal agreed between Britain and the European Union. The UK Safer Internet Centre has been extremely reliant upon grants it receives from the European Union and there is also relevant EU legislation, such as the e-commerce directive, which if amended could make our engagement with internet companies much more challenging in the future.

9.2 The UK Safer Internet Centre is co-funded under the Connecting Europe Facility (CEF) programme of the European Commission. As such we contribute to the Better Internet for Kids (BIK) core service platform to share resources, services and practices between the European Safer Internet Centre's and advice and information about a better internet to the general public. In line with the European Commission's Better Internet for Kids strategy, the key vision behind the BIK core service platform is to create a better internet for children and young people.

9.3 The UKSIC is also concerned about our relationship with EU agencies such as Europol, Eurojust and participation in the European Arrest Warrant, which could make it much more challenging to address cross-border crime issues such as those that we deal with online post-Brexit if a meaningful deal is not pursued on security collaborative arrangements.

11 May 2018

Michael Veale, University College London - written evidence (IRN0077)

1. I am a technology policy researcher at University College London, who has undertaken a range of research in automated systems and the law as it applies to topics of interest to the committee.

2. The large volume of content posted online has meant that the large social media platforms, such as Facebook, Twitter, and Google, have turned to automated systems to detect content that may be illegal, hateful or "toxic" to participation, and either to automatically remove it, de-rank it in priority, or flag it for manual review.

Issues with automatic content moderation

3. Automated content moderation systems are useful as tools, but can also be problematic. There are several major concerns they raise:

4. Firstly, these systems often require a great deal of human labour. Technology firms use large out-sourcing operations to build these classification systems. The human review process to understand what content is illegal and what is not can cause psychological stress for these workers, who generally receive few of the supporting benefits of workers for the organisation as a whole. Increasingly, it is reported that these workers are based in developing countries for reasons of economic efficiency. Just as the Fair Trade movement was concerned with the supply chain of labour in commodities such as tea and coffee, there may be a need to ensure that the working conditions for those who moderate content online, and train the machine learning/artificial intelligence systems to recognise what is illegal and what is not (e.g. violence and child pornography), are fair.

5. **Recommendation: Firms using artificial intelligence to improve their response to illegal and potentially traumatising content online must be transparent about working conditions of those training the algorithmic systems, subject to audits and held to account.**

6. Secondly, recent research from the University of Oxford and University College London has demonstrated the potential for bias in these automated content moderation systems, particularly when they are not looking for illegal content, but for harmful or "toxic" content.[1218] This can manifest in a

[1218] Binns, Reuben, Michael Veale, Max Van Kleek, and Nigel Shadbolt (2017) "**Like Trainer, like Bot? Inheritance of Bias in Algorithmic Content Moderation**." In *Social Informatics: 9th International Conference, SocInfo 2017, Oxford, UK, September 13-15, 2017, Proceedings, Part II*, edited by Giovanni number of forms, from different opinions from different societal groups on what counts as "toxic", to simply judging people on the way they write or speak, rather than what they say. Related work shows how grammatical constructions associated with ethnic minorities can be much more difficult for deployed algorithmic systems to understand than more mainstream language use, opening the door for discrimination.[1219]

7. **Recommendation: Firms using automated content moderation at scale must transparently demonstrate the methods by which they have tested, and continue to test, such systems for bias and discrimination.**

8. **Recommendation: A list should be maintained of particularly influential firms using automated content moderation who should deposit recent versions of their filtering architecture and systems in a publicly accessible repository, such as the British Library, for scrutiny.**

9. Thirdly, a goal of media regulation has often been to encourage diversity in content, both to better represent the public and to better encourage the clashing of viewpoints and the support of democratic engagement. Much moderation online, including filtering, does the opposite, creating "filter bubbles" or echo chambers which are difficult to break out of. This is problematic, and firms should be encouraged to ensure that they attempt **diversity-by-design**. Individuals should be able to understand how the world they see online might differ from that of somebody very different to them, and react to it.

10. Lastly, some uses of these systems might be illegal. The General Data Protection Regulation ensures individuals are notified of, and can challenge, significant, fully automated decisions.[1220] Yet it is not clear that many companies realise that censoring someone might be considered a significant decision, and that they must offer this right. The lack of clarification in the courts may be contributing to this uncertainty.

11. Furthermore, where firms are inferring political opinions to make censorship decisions, they are processing "special category data" (Article 9, GDPR). Under the GDPR, they are likely to require explicit consent. It is unclear whether they are aware of this obligation, which would apply not just when

Luca Ciampaglia, Afra Mashhadi, and Taha Yasseri, 405–15. Cham: Springer International Publishing, 2017. doi:10.1007/978-3-319-67256-4_32.

[1219] Blodgett, S. L., & O'Connor, B. (2017). Racial Disparity in Natural Language Processing: A Case Study of Social Media African-American English. *arXiv preprint arXiv:1707.00061*.

[1220] For more information, see Edwards, Lilian, and Michael Veale. (2017) "**Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For.**" *Duke Law & Technology Review*, 16, 1, 18–84. doi:10.2139/ssrn.2972855.

political opinions are expressly collected, but also when they are implicitly inferred.

12. **Recommendation: The Information Commissioner's Office should examine issues of online content moderation, and to what extent existing practices are in breach of Article 22 of the GDPR on automated decision-making, and Article 9 on processing special category data, including political opinions.**

13. **Recommendation: UK Research and Innovation (UKRI) should create a special fund to work with and support regulators, including the Information Commissioner's Office, on understanding the tricky social and technical issues underlying internet regulation.**

May 2018

Adrian Venditti – written evidence (IRN0002)

I believe that the greater risk for people lies in encrypted communication messaging services which conceal the text sent using secure encryption methods rather than plain text social media platforms like Facebook and Twitter. Covert messages sent between loosely-connected associates in an activist cell using encrypted messaging services like WhatsApp and Viber (further concealed using VPN communication technology which ensures a secure encrypted communication network for service users) allow people to form collective groups to achieve their aims without needing to meet in public gatherings. While Facebook and Twitter may have their limitations in terms of how quickly they respond to "takedown" or "cease and desist" notifications I feel that they do a reasonable job. Language analysis tools and multi-lingual language translation tools would be of use to Facebook and Twitter, and Facebook already offer language translation options for converting between different languages and I believe that can be leveraged to provide identification tools for the detection of individuals who are trying to radicalise other vulnerable people.

I think internet service providers have a significant role to play in suppressing the "dark web", an online environment where people may try to conceal their identity and activities such as money transfer using crypto-currency like bitcoin where concealment of the identity of the owner of the "ransomware" payment is guaranteed by the design of the computer systems that support bitcoin and associated crypto-currencies. Using an alias or nickname to hide your true identity on encrypted messaging services where identification is only based on the person's photo may mean the police and other investigators need to be trained in the forensic analysis of software installed on devices like smartphones and tablet computer, such as the signs of apps having been deleted from the device but data in the smartphone vendor App Store showing that there was once an app on the device like WhatsApp and possibly a linked account in the service. An example of what to look for is Apple computer software feature called "iCloud keychain" where login credentials are stored in central servers and can be used for logging in to websites. There's plenty of scope for covert communications outside Facebook and Twitter if people look hard enough, for example Apple iMessage service. I think the way forward on this is to seek advice from the product vendor (Apple, Google, Samsung, Blackberry or IBM) on what encrypted services are supported by their devices, regardless of being peer-to-peer messaging/voice calls over data service/text messaging over data service or document or file storage or sharing using cloud storage services such as google drive, Apple iCloud, Microsoft OneDrive, Dropbox. The smartphone vendors are the people to ask about the different categories of apps available on their devices.

3 April 2018

Virgin Media, Sky and TalkTalk Group – oral evidence (QQ 103-112)

Transcript to be found under Sky

WebRoots Democracy – written evidence (IRN0043)

1. WebRoots Democracy is a think tank focused on the intersection of technology and democratic participation. We have recently commenced a research project *Regulating Social Media* (RSM) which is exploring similar aspects of the Committee's inquiry. We organised a public seminar looking at this in April entitled 'Cambridge Analytica and the future of social media', a write-up of which can be accessed here. Our first report for the RSM project is called 'Kinder, Gentler Politics' and is focused on the rise of online abuse in political debate.

Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

2. Specific regulation for the internet is necessary and should be desirable in a society that believes that those with power should be held to account. It should also be desirable for those who support the idea of free speech which can often be plagued by unfettered online abuse. The most challenging question is whether any serious regulation can be implemented when the internet is a borderless, global entity and where the major players are based outside of the UK.

3. The internet is akin to a library in which nobody has a grip on the number of books coming in and out, never mind the content within them. In order to get a handle on this, it is clear that there needs to be an international effort and consensus on what an acceptable, free, and safe internet should look like. Limited legislative actions by the UK alone will not hinder malicious actors, or worse, malicious states, abroad. However, we can do more to better equip our population and educate them about responsible and informed internet use.

4. Compulsory digital literacy education in schools is something we have advocated in the past, particularly in the face of the so-called 'fake news' phenomenon. Adult digital literacy education is a policy we will be exploring as part of the RSM project. Other areas we will be looking at is the pros and cons of setting up a new UK regulatory body for social media platforms, as well as the level of resources for the police in preventing cyber-crime and tracking down offenders.

5. Regulation is certainly possible and doesn't have to necessarily reflect more extreme examples of censorship as seen in other parts of the world. The internet is a democratic ideal, but currently, a highly uncivil one. The topic of internet regulation is more a social and philosophical issue than a technical one. Does light-touch or no regulation bring about a more democratic and free space? Or do we need accountability, rules, and enforcement to ensure a civil society can be maintained?

6. Whilst we are not yet in a position to provide more detailed thoughts to the Committee, we are happy to share findings of our RSM project over the course of the next few months.

11 May 2018

Which? – written evidence (IRN0116)

Introduction

Which? has recently undertaken an investigation into the consumer data landscape, with the goal of understanding how far consumers may require further support to rebalance power of the use of their data. We carried out in-depth original consumer research on views and attitudes to personal data use, and published our findings in a report, *Control, Alt or Delete? The Future of Consumer Data*, in June 2018.

Digitisation and the use of data about our consumer lives has already brought huge benefits and great potential for empowerment. Our research found that many people feel powerless to understand either the growing commercial observations or the effect that accelerating data collection is having on their lives. We want to see a world where consumers are empowered by digital advances but we think that the current level of understanding and comfort with data use is not a sound foundation. Companies and Government need to take consumer unease in this area seriously, and we make three recommendations in our report:

- Consumers and their advocates need more transparency about the impact that personal data has on their lives.

- The Competition and Markets Authority (CMA) should conduct a market study in to the digital advertising industry as a matter of urgency.

- It is time for a thorough review of governance of data in motion, with due attention given to creative ways to improve oversight and enforcement.

Our research is particularly pertinent to the following three questions the Committee has posed in its call for evidence.

What information should online platforms provide to users about the use of their personal data?

Consumers usually judge the acceptability of data collection and use by the impact that it has on them; for example whether it is having an influence on the products and services displayed online, on discount offers they receive, or on access to products such as insurance or credit. In many cases consumers are either not given this information at all, or are given it out of context at the time of sharing data, rather than at the point the data is used. Many consumers are therefore forced to make decisions about sharing their data with only a partial picture of the impact the decision will have. To tackle this, it is important to consider both how and when the information is provided.

Which? is calling for businesses, including online platforms, to do more to inform consumers of the impact that the use of their data has on their lives at the time it is being used (for example, when an insurance quote is being given) when this is possible. Where it is not possible to do this on an individual basis, the Government, as well as regulators, businesses and civil society, needs to focus on understanding the impacts of data usage on people's lives.

Our research also found that consumers need to be able to trust the governance of the data ecosystem if they are to engage with it confidently, so it is important that a trusted system of data sharing is established that allows innovation but also improves the ability to provide oversight and enforcement.

Our report sets out a series of recommendations of actions in these areas. Specifically:

- Companies need to consider how they can ensure people understand the impact of the use of their data, at the time they are transacting with them.

- The Centre for Data Ethics and Innovation (CDEI) should prioritise understanding the impacts of personal data use. They should also undertake a thorough review of the governance of data in motion (alongside the Information Commissioner's Office's (ICO) planned work on credit reference agencies and brokers), with due attention given to creative ways to improve oversight and enforcement.

- The Competition and Markets Authority (CMA) and the Department for Business, Energy and Industrial Strategy should conduct a programme of work to investigate the impacts of data use on consumer markets.

- The ICO should explore the impacts of data usage as well as the legality and processing, particularly how the GDPR provisions on profiling are being put into practice to see whether they could realistically tackle the lack of consumer knowledge that we have identified.

Our research shows that people recognise that the collection and use of consumer data has brought huge benefits and great potential for consumer empowerment. However, many people feel powerless to understand the effects that accelerating data collection is having on their lives. For example, eight in 10 consumers are concerned about organisations selling data to third parties, even when it has been anonymised, and many consumers are not aware that their data can be amalgamated to form a complete individual level profile.

The sense of powerlessness appears to arise from a combination of factors including:

- People lack knowledge about the full extent of personal data collection and use;

- Data-driven technology has become central to people's daily lives, which means they feel they cannot give it up; and

- People perceive a lack of alternatives if they want to stop using specific companies whose data collection practices they might be concerned about.

Many consumers therefore choose not to engage because it does not feel worthwhile; it is difficult to do so and there are few options available in any case. It is therefore important that businesses provide consumers with more transparency on the impacts of data use and the Government and others must work together to understand these impacts.

The lack of understanding of the impacts of data use both on society and for the individual makes it difficult for organisations like Which? to determine where harm is occurring, what can be done to empower consumers, or to understand fully the true impacts that data use is having. Which? is calling on the CDEI, CMA and others to work together on this complex and important issue, and involve external stakeholders including Which? in coordinating action. We recently submitted responses to consultations by the ICO and the CDEI in which we highlighted the vital role that they have to play in improving transparency of data collection use and its impacts on consumers.

In what ways should online platforms be more transparent about their business practices - for example in their use of algorithms?

Increasing transparency about the impacts of the use of consumer data is important for empowering consumers in the digital landscape, particularly where an impact might be to exclude them from access to products or services or change the prices they see. Where it is possible, we want to see companies providing users with *transparency in context* about the use of their data in real time and when it is occurring so that they can understand how the data held on them affects their lives. The impact on their lives is more important to people than whether a particular computational technique has been used.

As noted above, where these impacts can be hard to communicate on an individual basis, we want to see government, regulators, businesses and consumer advocates working together to understand the impacts of data usage.

Our research shows that consumer attitudes to data are often pragmatic – they are willing to share their data if it is relevant and they understand the benefit that they (or society) get - for example, when the data shared is used to provide personalisation and new innovative products. However, people become concerned once they are given more information about the full spectrum of data collection practices and how that data may affect what they see and the choices they have. For example, many consumers are surprised that unknown companies ‘profile’ them as an individual and they are uneasy about the use of data science to infer aspects of their which could be used to target them in potentially harmful ways without their knowledge. Vulnerable consumers in particular are concerned about the direct impacts that the use of their data could have, including how ‘irrelevant’ data could be used ‘against’ them.

Profiling at an individual level, and ‘micro-targeting’ on that data, can create the potential for various types of consumer detriment, including financial harms, non-financial harms such as discriminatory access to information or services, or lower uptake of digital services due to consumer concerns.

For these reasons it is important that consumers fully understand the impact that the use of their data has on them. The current lack of transparency means even extensive efforts cannot give consumers straight answers to the questions that need answering. Companies therefore need to consider how they can ensure people understand the impacts of the use of their data, at the time they are transacting with them and that consumers are fully informed about the practices that arise from the data that their online activity generates.

What is the impact of the dominance of a small number of online platforms in certain online markets?

Nearly all online business models rely on data to facilitate transactions, but many also use it to generate revenues through targeted advertising. The use of consumer data has enabled innovation and delivered benefits in the form of greater choice and often lower prices and better quality services. However, the way data is used has also led to privacy and competition concerns.

In many areas of the digital world vigorous competition exists. However there are some areas of the digital landscape where the dominance of a small number of companies could cause problems for consumers. Our work in this area has focused on those areas where the *collection and use* of data itself can create a competition issue. One of the primary manifestations of this is in the digital advertising industry and the practice of ‘people based marketing’. This market is largely concentrated in Facebook and Google’s hands (we have quoted sources in our report that suggest they commanded 54% of the UK digital advertising market in 2017 and 59% of the global market) and this domination is only likely to increase. Which? is calling on the CMA to conduct a market study into the digital advertising industry so that its impacts and consequences on consumers can be fully understood, and to understand whether the concentration of the digital advertising market in Google and Facebook’s hands is harming consumers through supply chain impacts. We note that the Committee also called for such a study following its report on UK advertising in a digital age.

Competition in online advertising has recently come under scrutiny in various jurisdictions, such as sector-wide investigations in in Australia, France and Germany. In 2018, Which? commissioned Oxera to produce an economic paper that explores how the use of consumer data affects consumers across a broad range of markets through competition and privacy outcomes. It describes the harvesting and use of consumer data as central to the competitive strategies of all players and that domination in digital advertising can affect consumer outcomes in two main ways:

1. a large vertically integrated platform might be able to set higher prices or offer lower-quality services to advertisers, for example by artificially creating scarcity of possible ad placements.

2. a vertically integrated platform might be able to foreclose competitors by refusing access to its systems by limiting interoperability or forcing competitors to incur (prohibitively) high costs to obtain the same consumer data thereby hindering competition.

Both of these concerns could cause harm for consumers through higher prices for advertised goods or lower-quality advertising, although the current empirical evidence that this is occurring is limited. Additionally, the dominance of one or two companies means that consumers often feel they do not have viable alternatives. For example, 24% of those who we sampled and who used Facebook said they considered leaving the site following the Cambridge Analytica revelations, but did not. Only 6% actually said that they deactivated or deleted their account.

The continuing growth of the digital advertising market will only exacerbate competition concerns. The industry is complicated and opaque, making it difficult for consumers and their advocates to understand the impacts and consequences or provide good public information about what is happening.

October 2018

Which? – oral evidence (QQ 161-173)

Tuesday 23 October 2018

Watch the meeting

Members present: Baroness McIntosh of Hudnall (Chairman); Lord Allen of Kensington; Baroness Bonham-Carter of Yarnbury; Baroness Chisholm of Owlpen; Viscount Colville of Culross; Lord Gordon of Strathblane; Baroness Kidron; Baroness Quin.

Evidence Session No. 19 Heard in Public Questions 161 - 173

Examination of Witness

Caroline Normand, Director of Policy, Which?

Q161 The Chairman: Ms Normand, thank you very much for coming to speak to the Select Committee on Communications. You should know that the meeting will be broadcast online and a transcript will be available in due course.

I am going to ask you the first question but I wonder if, when you answer it, you could wrap in just a bit of background about yourself—wrap with a W, not with an R, by the way—and tell us anything you want us to hear by way of introduction. That would be very helpful. The first question I wanted to ask you is about the strengths and weaknesses of the regulatory framework of the internet that currently exists in relation to protecting consumers online, and whether the current regulatory bodies, in particular the ICO and the CMA, with which I know you are very familiar, are effective and properly resourced. Can I ask you, since it has come up recently, whether you could include in your answer some comment on recent research from Which? on fake reviews? That would be of great interest to the Committee.

Caroline Normand: We very much welcome the opportunity to assist the Committee in this inquiry on what is a very important issue of the day. Which? is a completely independent charitable social enterprise. We have over 1 million members and supporters, and our mission has always been to make consumers as powerful as the organisations they deal with. Obviously, increasingly today the way in which we interact with those organisations is digital. Our recent focus has very much been on how business accesses personal data and how that has changed the consumer world.

We know that digital markets and greater data flows have brought a great deal of good for consumers, for individuals. Shopping is more convenient, we can all book holidays online, we have greater choice, we can manage our fitness, and indeed we can even control specific health problems, from diabetes through to cystic fibrosis; there are some great online communities that are really helping people. However, we undertook a large programme of research for our report, *Control, Alt or Delete*, and we found that while people love technology, when you start to talk about data they are much more conflicted. They are conflicted about who and whether to trust the data ecosystem that operates the online market. We found a widespread sense of disempowerment and disengagement among individuals, with many people unsure about the impact that data use has on them, or whether it is worth doing anything about it when there are practices that they do not like.

From our perspective at Which?, we do not think that is a sound foundation for the future. From our perspective, yes, we think that more regulation for some aspects of the online world is definitely needed, but, going back to my first point, it has to be considered regulation. Herein lies one of the big problems that we faced in trying to do our report, because the deficit of transparency about the system is a huge hurdle in understanding what is going on, what the problems are and therefore what the right and appropriate solutions are.

In the light of our research we made a series of recommendations calling for, first, companies to provide much more transparency about the impact of data use on individuals at the time of use. People did not talk to us about privacy concerns; they talked to us about, "How is my data being used? What is the impact on me? What is the impact on my credit rating or on my insurance quote?" That is what they wanted to know. Complementary to that, we think that Governments and regulators rapidly need to understand more about the impact of data use at a global level. That is the first recommendation.

The second recommendation was around the flows of data. Something that really struck us from our research with consumers was how much they disliked data-sharing or data being sold, even though that is the way in which the system works. Over 80% of people we spoke to were concerned about data-sharing and data flows. It is very hard to reassure people about how the system works if you do not know what the governance framework is for said data flows. We think that the Centre for Data Ethics should conduct a review of data in motion, to understand how the flows of data work, to make sure that any regulation is fit for purpose.

Our final recommendation, which will be familiar to you, is that the Competition and Markets Authority should conduct a market study into the digital advertising industry, looking both at the concentration in the industry, which is something that drives the ecosystem of the industry, but also at the impact of digital marketing on people's lives. That is what our report recommended.

As our research showed, the voice of the individual and the consumer is pretty lost in this space. We think that that is another aspect of this environment that needs to be looked at, both by the dominant players, the players in the marketplace, but also by the Government. There is a really strong sense from individuals that they do not really know where to turn and have no redress when things go wrong. It may be that, when there is a security breach or some other event happens, people are informed about what to do, but they do not have the trust or feeling that they are, and that whole environment is not really there.

Finally, another final and important aspect of this is that, while it is encouraging to see all of the activity looking at this space and playing catch-up and trying to understand what is happening and what, if anything, needs to be done to improve the experience for consumers and others, it is very confusing in its own right. There are lots of initiatives, there are lots of regulators, there are underlaps and there are overlaps. We think that that needs to rapidly be sorted through, so that we have the appropriate level of regulation and the appropriate regulators as quickly as possible.

Your question was whether the regulators are appropriately resourced. This is a huge challenge. The speed and scale of change in the digital world is enormous and is difficult for regulators to keep up with. It is very good to see that the CMA has its new data unit, and we look forward to seeing some of the outputs from it. We need to make sure that that work is properly resourced and does not suffer in the light of all the extra work that will come to the CMA from Brexit.

There are huge challenges for the ICO just in keeping up with the skills and the understanding compared with those that they are regulating, and that is a challenge that other similar regulators around the world face as well. It is one of the big challenges for regulation of the day.

As I have said, it is not all just about resourcing. There are also some challenges about co-ordination, between regulators and the Government, and who does what and how. That is not just the ICO and the CMA, but economic regulators like Ofcom. Ofgem is thinking about a number of data issues relating to consumers, but also vulnerable consumers, and that level of co-ordination is, at the moment, lacking and needs to improve.

There are questions also around transparency. For example, the ICO should publish more details about its work on some issues like data-brokers, so that we can understand more about what it is learning.

There are some final issues that are more generic, but are important, in relation to consumer enforcement, which have been highlighted in the Government's consumer Green Paper around the landscape of consumer enforcement as a whole and how we make sure that is as effective as it can be, potentially with a greater sense of leadership in the centre, possibly for the Competition and Markets Authority, and greater powers for some organisations like the CMA to be able to issue fines where there are problems for consumer enforcement, so that they can provide greater deterrents quickly, which is particularly important in an area like this, which moves so fast.

Q162 **Lord Gordon of Strathblane:** You made a point about who regulates and what—could I add in, "and how quickly"? It appears that there is a major problem in that if a statutory body recommends to Government that there be legislation, frankly, by the time the ink is dry on the legislation the game has moved on. How do we cope with the internet? How do Government cope with it?

Caroline Normand: It is a big challenge. The speed with which things are moving at the moment is very challenging. I do not think that means you give up and you stop before you begin. Obviously there are different types of tools and different types of investigation that different regulators can use. I have just mentioned the CMA's ability to issue fines for consumer enforcement matters, and not just the current recourse they have to the courts. That is one way that you could speed things up.

In relation to the way that competition cases and other things are conducted, there are ways in which we would like to see some of those cases being prosecuted as fast as possible, but we are in a world where things are moving quickly.

Lord Gordon: Is there not a case for Government to have somebody employed, at a fairly senior level, to guess what is coming next, so that we are ready for it when it comes, rather than reacting all the time to things that are already in place?

Caroline Normand: That is one way of addressing it. The only other thing I would point to is that in other areas—for example, in the communications area more broadly or in the energy area—you have consumer panels, you have means of understanding complaints that are coming in and you have consumer bodies, ombudsmen and others who can translate the complaints back to the regulator to see what is happening in real time. We do not have that kind of a mechanism at the moment working well in the area of the internet more generally. That kind of early warning and real-time issue that people have is not getting through the system easily and readily.

The Chairman: You have talked about a number of different regulators, and you are obviously worried that there is not sufficient co-ordination between those different regulators, irrespective of whether they have enough power or enough resource. To follow up on Lord Gordon's question, is it any part of your view that we are missing another regulator to regulate the regulators?

Baroness Bonham-Carter of Yarnbury: It sounds like a backstop backstop.

The Chairman: To put it another way, is there a co-ordinating body, rather than an individual, that should have the job of making sure that that joining-up happens?

Caroline Normand: There are a few answers to that. I do not think that the regulators at the moment, or the levels of power, necessarily fit together well. Some of that is because some of these bodies are just recently set up, and some of the problems are relatively recently being understood. I do not have a blueprint for how those regulators and those bodies should fit together, other than to say that they should fit together better. I am not sure that creating another body over the top is necessarily the right solution. One could argue that, to a certain extent, the Government should be providing that overview, coming from DCMS.

I would point out, sitting where we sit in Which?, that it is quite hard to understand who is doing what, with what powers and therefore who to go to in order to try to solve things. My observation is that sometimes we find that we have bits of recommendation going to a number of bodies, and we are relying on them to co-ordinate between themselves in order to understand what is going on.

Q163 Baroness Kidron: I want to pick up on two things. They both relate to things you have already said, so you have partially answered them. If, instead of trying to invent the new, we were to rely on existing consumer laws and principles, but then we did the piece of the puzzle that you have already alluded to, which is to have some transparency, would those principles and laws, effectively and robustly applied, give you a lot of the levers that you need? We could bring the digital world into our existing understanding of consumer law, rather than trying to reinvent something new.

Caroline Normand: In relation to consumer law—the part of the law that is really around consumer protections—the consumer protections should be more or less at the same standard whether you are online or offline. If you buy food online or order a washing machine, et cetera, you should expect that you will be covered in the same way that you would be if you buy from the high street. Those protections are more or less in place, and in certain places you actually get more protection online because of what I was going to call the distance selling regulations but which, translated into the UK, are actually the consumer contracts regulations, which allow a bit more time, cooling-off-period time. In the sense of purchasing there are a number of consumer protections in place. In fact, the UK, with the Consumer Rights Act, has itself been innovative in having protections for digital downloads, so not just goods and services but digital goods.

There are some caveats. Consumers, when they are buying something, need to know whether they are buying from a trader, so a business, or whether they are buying from an individual, where their rights will not be quite the same. That is an important distinction for people to know when they are buying things.

When we are talking about consumer protections—I am very much in that world—there are two particular places we would highlight as concerns for us. The first is about purchasing online where you may be purchasing from another jurisdiction. It is difficult to return goods to enforce your rights, and at the moment there are a number of conventions that work with the EU that allow people to prosecute and to get their rights in the UK, even if they buy from a company in another jurisdiction. What will happen post Brexit is not clear, so it is something we are concerned about, to make sure that that is as easy as possible.

The second area—and I can also bring in the fake review piece—is just a concern about the prevalence of unsafe products that are sold online, and whether platforms are doing enough to protect people from these. As part of our campaign on potentially unsafe products, we have made a lot of progress on issues like CO_2 alarms, where over 250 listings were removed from Amazon and eBay. We also had experience with the children's toy slime, where all 11 products we found to contain unsafe levels of boron were removed by Amazon. They were as a result of our having done the testing. We are concerned that we regularly find unsafe products for sale online.

At this point, it is also worth bringing up our fake online reviews investigation, which you will have heard about, where our investigation has revealed how easy it can be for some sellers to bypass rules to offer free products in exchange for false and highly rated reviews. We think it is an area that the CMA in particular really needs to keep a lid on and make sure it is enforcing the rules appropriately, so that we see deterrent action taken against this kind of fake review.

Q164 Baroness Kidron: That is a rather nice segue into my second point, which is that actually what you are saying is that, within reason, the idea of the product itself is being dealt with, could be dealt with, with these caveats. The other area we are really interested in is the relationship between the user and the service. You talked about data and we are interested in whether terms and conditions are an unfair business practice, for example. One of the things that is frequently mentioned is that there is no opportunity to pay instead of giving your data, so your data does become currency. I wonder whether you can talk a little bit about what your feeling is about the flow of data in that regard. Are the sorts of deals that are out there fair on the consumer?

Caroline Normand: The question of whether consumers could pay, instead of getting product for free or access to services for free, is potentially fraught with difficulty. The example I have here is of the *Washington Post*, which has a premium EU ad-free subscription. This idea is starting to be experimented with. There are a number of risks that come with it. The first is that if you can afford it, you can protect yourself, in so far as that is the appropriate language, from data flows, and if you cannot, you cannot. We know from our research that it is often people who are most vulnerable who are most worried about where their data flows, so that does not seem to us to be a potentially good outcome.

Looking at it the other way round, there is the experience of Facebook in India, which you may have heard of. It is looking at the experiment the other way around. They offered something for free but restricted it. The backlash from people shows that this will only go so far with consumers. Companies should think about those things with care.

The realistic position on this one is just where consumers are, so they may be worried about data flows and they may be concerned about what can happen with those flows, but there is quite a sense of resignation and rational disengagement that goes on with consumers. That is maybe because they do not think there is anything they can do; it is sometimes because there are no alternatives to the services they are using, so even if they are concerned, there is not much that they can do about it; it is sometimes because they think that the horse has bolted and their data is all out there anyway, so what is the point? There are a number of questions that may mean that, even if those services were provided, very few people would take them up.

Baroness Kidron: If I could quickly pick up on your other point, where you said we should be more concerned about impact, do you think that, where the impacts are negative, the people providing the service have a responsibility?

Caroline Normand: If we understood more about impact, and if it was more transparent, what the impact was, it would allow us, business and consumers, to know whether to trust or to think that the thing that they were being offered was fair, which would allow people to take more choice. Let me give you an example of, say, an insurance quote. If you know what that insurance quote is built on, you will have a better idea about whether you think that is an appropriate quote, whether it is fair and whether it is one you will stand by. In those actions by a consumer in relation to that, no doubt, depending on what consumers decide to do, business will adapt.

Baroness Kidron: Equally, regulators will be able to see?

Caroline Normand: Exactly. Regulators will be able to regulate. The transparency would then allow the practice to be out in the open air, such that you can do something about it, whether it is the consumer, the business or the regulator.

Baroness Quin: I wanted to pick up on something you said when you talked about the pressure that you had put on Amazon and others to make redress and take off certain things that they were advertising. What sort of length of process was involved with that, from your making representations to their taking action?

Caroline Normand: I do not have the specifics with me today, so I am very happy to write to you with a sense of how long it takes. I do not think it is a very long and lengthy process per se, but obviously we have to test the products, then we have to do the discussions and then the products get removed. It is going to entail a certain length of time because of the necessity to test the products, but I will come back to you.

Q165 Baroness Quin: I would just like to know and see whether it is something that we need to have any concerns about.

My question is about the responsibility of consumers themselves, given that consumers are a huge range of people and some of them are vulnerable in this area, without any doubt. What responsibilities do you feel that consumers have for looking after themselves and protecting themselves from online crime or whatever? If they have got responsibilities, how can they best be empowered to be able to assume those responsibilities effectively?

Caroline Normand: My answer to that would be that consumers have responsibility where they are best placed to control the risk that they are facing. In many instances of online business, it is the business that will have much more knowledge and tools to control the risk than the individual does.

I will give you an example of the 2016 super-complaint by Which? on bank transfer scams, which we made to the Payment Systems Regulator. Which? set out evidence showing that if banks faced different incentives, the protection for the consumers against these authorised push payments—this is where consumers are scammed into transferring sometimes very large sums of money—the outcome for consumers would improve. What we have learned since then is that scammers have a range of extremely sophisticated techniques to identify and deceive consumers. In our strong view, banks are best placed to take systematic action to reduce this risk. The same must apply more broadly. This is a specific one, and it involves large sums of money, because it is in relation to banking, but the same principle must apply for other online businesses.

I have already mentioned the question about where you go when things go wrong, but let me come back on to how you might empower consumers to help themselves a bit more. First, there is not an obvious place for people to go and there is not an obvious point of help and resource and redress, so obviously they turn to people like Which?. Quite rightly, we provide people with advice around their rights, through our consumer rights website, to help them be aware of scams, the latest types of scams and how to spot and report them. We cover the differences between scams, rip-off deals and all of those sorts of activities that take place online. We also advise on the likely targets of scams—often things like investment scams will be aimed at retirees—and how to make a complaint to whoever you need to make a complaint to. We provide a lot of information.

Another thing that is worth pointing out is, even when an individual is proactive and does something about the problem, what happens. Our research last month found that over 96% of the cases that were reported to Action Fraud, which is the UK's fraud reporting centre, go unsolved. Less than one in 20 crimes handled by Action Fraud result in a suspect being charged, cautioned or dealt with in the justice system. We provide information about scamming but scammers are sophisticated. It helps up to a point. As I said, companies are often better placed to understand, and when consumers go to the place that exists for them to go to, it is not at all clear that much happens.

Baroness Quin: The obvious question then is what Government should be doing about those statistics that you have quoted, and I suppose the EU and so on. It is all very well consumers coming to you with their concerns, but it sounds like there needs to be some kind of much more effective enforcement mechanism at some level; I am not quite sure which level.

Caroline Normand: We argue now, and we have argued in the past, that there need to be much more effective systems of redress for consumers across the piece. Obviously there will be different types of redress for different types of activity. Here I am talking about scamming and fraud, but it is a real problem and online there are potentially many ways in which scammers and fraudsters can operate.

The Chairman: Could you just tell us, briefly if you could, whether it was clear to you, when you looked at those statistics, what it was that was preventing these things from being taken forward? You are talking about criminal activity here in the main. Was it lack of evidence? Was it lack of resource in the investigating bodies? What was preventing those things from being taken forward?

Caroline Normand: I do not have that information here. If we have it, I will certainly let you have it.

The Chairman: Thank you. If you could write to us with any other information you have, that would be very helpful.

Baroness Chisholm of Owlpen: Do you feel there should be a thorough review about enforcement and where people can go to get redress when there has been a problem? Do you feel that is what is really lacking at the moment?

Caroline Normand: Across the space that individuals and the consumer would regard as the internet—because people think in the terms that they think and consumers will think about this being online—it is not at all clear where people go and can go. There will be different places that will take different types of action. Obviously the ICO has some powers, there is Action Fraud, and there are things in between. How they join up, what the impact is, what the effective outcomes are, and, critically in the middle of this, what the redress for the consumer is is not entirely clear. Some of these enforcers will enforce in order to right the wrong or to prosecute the individual, rather than to provide redress to the individual consumer. There is a range of issues in this space that I do not think are well understood, and I do not think they contribute to the trust that people have in the system and what I have already described about data flows and so on.

Q166 Viscount Colville of Culross: I wanted to ask about the design of algorithms. Should we be legally requiring the tech companies to open up their algorithms, even if they are commercially sensitive, which is obviously the objection, or should we just be concentrating on the decisions that are made by the algorithms so that they can be challenged properly?

Caroline Normand: From our perspective, and what we heard from consumers, the key thing is what the impact is, so what the outcome is. From a Which? point of view, we are always interested in the outcome on individuals. We are interested in the outcome in terms of what comes out of an AI decision, if you like. From our perspective, that is the most important thing. If that requires transparency and opening up how the algorithms are constructed, maybe it does, but from our perspective the outcome of those decisions is not well understood, and that is where we would start.

Viscount Colville of Culross: How would you enforce that?

Caroline Normand: I am not at the enforcement point. I am at the transparency point. We are back up the line. Our observation on trying to do the work that we did was that we need to understand what is going on before we can enforce things, and it is not transparent. It is not understood where algorithms are being used and what the impact of those decisions are. I go back to the point I was making about the impact of use at the time of use. That is one device by which you could get at some of the outcomes of what is happening from algorithmic decisions. I just reiterate that an organisation such as Which?, a consumer body, has tried quite hard to understand what is happening, but there is really not much transparency when trying to get to grips with this. That is why I am going back up the story, because individuals do not understand this either.

Viscount Colville of Culross: That explanation of how the decision is made, in your view, should be very clearly laid out, so that the consumer can understand what the effect of the algorithm has been in that decision.

Caroline Normand: I am sorry if I sound like I am repeating myself, but what the consumer wants to know is, "Why am I seeing what I am seeing?" It may well be that at the moment it is quite challenging to answer that question on the back of an algorithmic decision, but that is what the consumer wants to know. They want to know why they see that advert, why they get that credit score or why their insurance quote is this. We have had scare stories in the past, right or wrong, that people with Hotmail addresses were getting more expensive insurance quotes than people with Gmail addresses, for example. Whether true or not, it is an example of the kind of thing where people would just like to be sure they understand why they are getting what they are getting.

In understanding that, that then forces questions around, "What is behind this decision? What went into the algorithm?" It is quite likely that this is not well understood by the companies operating all the decision-making, because obviously this is a quick way of getting to decision-making. It poses its own challenges when you look at the final outcome and say, "Why?"

The Chairman: I will ask Lord Allen to add his question at this point, because it might give you an opportunity to unpack this issue.

Q167 Lord Allen of Kensington: This leads on from what you have just been discussing. I was particularly interested in your written evidence regarding things like individual profiling and micro-targeting. It specifically is around a risk of algorithms being used to discriminate in terms of pricing, so, whether it is Baroness Kidron or myself, you could have data that may suggest that we would respond differently to different levels of pricing. That is a fairly obvious issue. The question is whether you have any thoughts about what could be done about it?

Caroline Normand: On the personalised pricing point, we did not come across any evidence of specific personalised pricing of the type where, for example, a pen costs more for one person for some reason compared to someone else. Obviously across marketplaces and elsewhere, differential pricing is something that you see, and sometimes we are happy with it; sometimes it is the way in which markets operate, whether it is because you are encouraging new entrants by vouchers or something. Sometimes we are not happy with it, because it is targeted at vulnerabilities or it is targeted at people's inertia or misbalance in information, and so on.

Lord Allen of Kensington: I can understand the demand and supply thing. If you look at it with airlines, we all pay different pricing on the airlines, so I can understand that. The specific targeting of individuals and discriminating against them is the area I am trying to unpick a little bit.

Caroline Normand: No, I understand. I am afraid this argument is a bit circular. What we need to know is what has gone into the targeting of individuals and the pricing decision that they are seeing, or the voucher or the deal that they got. Why have they got it and what has gone into the decision, AI or otherwise, to get them to that point? That is what is not understood, and that is what is not known.

Our response to that is, "Tell us what went into the decision so that we can see what you have used. What about the individual have you used in order to come up with that price?" That could in turn mean that the wrong pieces of information have been used about the individual, or inappropriate pieces of information—for example, an email for a credit report. It could uncover instances where profiles have been made about individuals, and used, that are inaccurate. That is another thing that concerns individuals. In that world where profiles are constructed, if you trace back through or do an information request you can find that sometimes those profiles are remarkably inaccurate. That has its own problems.

Q168 Baroness Kidron: I think I know what you are saying, but maybe it would be useful to hear it this way round. There has been a lot of concentration, particularly amongst people like us, on AI. What you are saying is that you do not care how you get there so long as you can tell the story in words. What you want is a list of attributes that made a material difference, not some magical formula.

Caroline Normand: I am going to hesitate on the word "list". Essentially what we are looking for is some means for individuals to understand why they are seeing the thing that they are seeing or the result that they have got. They need to be able to understand where it comes from and what has gone into it. Those are the things that they need. We are not expert in this, and we know that consumers do not want reams and reams of information, because they will not read it.

Having said that, Google has started to have a go at this in some areas, in providing a bit more information about where ads come from; you can press a button and you get a bit more information. Let us not forget that these companies have invented the digital advertising market, which puts adverts in front of your eyes in milliseconds. I do not claim to have all the answers, but I also do not think it is beyond the wit of the companies that we are talking about to start to think about it more seriously. It is a really important thing in order to build the trust that is required to make this thing continue in a stable and solid form.

Q169 Baroness Bonham-Carter of Yarnbury: Going slightly backwards, Which? was established in order to champion consumers in a very different world. We were talking earlier about whether the regulatory framework needs be beefed up, or changed, or whatever. You also said you are not expert yet, but is there a place for a more technological version of Which?? I know you do your reports and stuff. We are all agreeing the consumer is in the dark, so I am trying to go backwards to the original conception of Which? Is there an opportunity for something like Which? for the modern world, or is it just too much beyond? I do not mean Which? itself; you know what I am trying to say here.

Caroline Normand: I do, but I am nevertheless going to respond and say Which? is very much for the modern world. This report that we put together is a no-brainer. We have to understand this better. It is just challenging. We are not alone. We are not the only people trying to understand what is going on; there are many people doing that. We are absolutely in this and for it, and need to, but we will never be technology experts. We will never be at the cutting edge. We will do what we need to do, and we need help in the form of greater transparency, in order to help do our job. That is one thing I will say.

At the beginning I did say that there are a number of other regulators around the space that have been invented a number of years ago, because we had energy suppliers, we had communications and so on, who had the benefit of more information around the problems that consumers face, whether it be complaints or understanding from a consumer perspective. Our observation is that is not present at the moment in the digital sphere. There is a good question as to whether it should be, but Which? will be there.

The Chairman: In the modern world.

Caroline Normand: We are in the modern world, and we will be doing our job.

Baroness Bonham-Carter of Yarnbury: I was not trying to suggest you were not. I was trying to suggest quite the reverse. I was suggesting that maybe you are very much part of the answer. That is what I was trying to say.

Caroline Normand: Indeed we are.

Q170 Lord Gordon of Strathblane: It seems to be almost inevitable that companies that provide a service on the internet acquire market dominance of the field totally. Once you get to 51% to 49%, it is a fairly rapid run to get to 90%-10% and total market dominance. Do you think it is inevitable or is there anything we can do about it, or can we mitigate any harmful effects?

Caroline Normand: There are a lot of areas of the digital world where there is a lot of competition, often in the early stage, but there are a number of areas where competition is vigorous and exists. Equally, as you say, the tale rapidly grows into some very large companies who dominate. There is some really interesting work that Oxera did for us around some of those questions around dominance and around the role that data plays within it. For example, your access and your ability to get hold of data, the cost of acquiring it and the depreciation of the data mean that there are some types of data that are much more precious.

Lord Gordon of Strathblane: Do you mean time-sensitive data?

Caroline Normand: I mean time-sensitive data or data that is hard to get hold of. That might help dominant companies more than some other types of data. For example, it is not that hard to get hold of people’s age, their addresses and so on. It is quite hard to get hold of the sorts of data that you might have through messages and what people write about. That is much more time-sensitive and much harder to get hold of, so there are some interesting questions that come into play around dominance, what causes dominance and what can help people to stay dominant.

Those questions on data raise, as you will well know, many new issues for our competition authorities. How does your assessment of market power shift in light of how much data you have of different types? How does it shift in relation to the networking effects that you have from the different services that you offer and the number of people who connect into you? There are interesting questions in merger cases: how do you look at the acquisition of a pretty small company, for example, that might not even make the merger thresholds but that holds a lot of personal data? All of those things are important. We are very pleased to see Professor Furman’s review that HMT is conducting, because we think those are very important things to get right and to start to develop, so that they can work in practice and not just theoretically.

I would go on, and I do not need to repeat myself, but in particular we think that the digital advertising market, and the dominance of two players in that, is a particularly important part of this, just because it drives so much of how the system operates.

Lord Gordon of Strathblane: In a way, it could also be argued that it enables the company to provide a better service, having more complete information. It is a question, perhaps, of evening up the balance. Do you think that data portability would help even the balance slightly in favour of the consumer?

Caroline Normand: Data portability is an important right in GDPR, and it has pretty significant potential, but it requires certain conditions. The one that I would underline the most is that people need to trust in order to be happy to adopt data portability. The sorts of concerns that they might have about data-sharing and security are really important things in order to make sure that data portability can work. In addition to that, our experience to date is that there needs to be a certain degree of mandation. So, for example, the experience of my data, in energy, which was based on a voluntary standard, took many years to get anywhere, and I question whether it has. Obviously, open banking was mandated through PSD2, and therefore mandated open APIs has allowed that to develop more quickly.

Having said that, and going back to my first point, we are seeing that play through in open banking. There is a question of awareness, of course; I think only about 28% or 30% of adults were aware of open banking in August, which is about eight months after it came in. At the same time, 77% of people said that they were concerned about allowing companies other than their main bank to access their financial data for security reasons. In the data portability world, if it is going to be used for switching, for new services and for innovation, people need to be comfortable and to trust in order to use it, and that takes me back to some of the points I was making earlier about trusting where your data flows to, what the appropriate governance framework is for the way in which data flows and where it stops. Does it stop?

The Chairman: We are approaching the witching hour for the Committee. As you see, we are about to start haemorrhaging members. I am going to ask that Lady Chisholm's question, which she is about to ask you, is the last; and ask you, if Lady Quin is content, to write to us on the subject of the impact of Brexit—which we always come to at the end of the Committee's proceedings. If you would be kind enough to write to us with any thoughts you have on that, we would be very grateful. In the meantime Lady Chisholm will ask her question.

Baroness Quin: Could I add a rider to the Brexit question? You said what you think the effect of Brexit is. I would be interested in how you see the role of Which? working within the European consumer networks, which I know have been very important over the years. I would like to know whether you see that continuing after Brexit and, if so, how?

Caroline Normand: Absolutely.

Q171 Baroness Chisholm of Owlpen: As we know, there are widespread concerns about the ethics of data collection, and, indeed, you mentioned earlier how the consumer's voice is lost in that. Do you feel that for them to have meaningful control over their data after it has been gathered we need change in regulation?

Caroline Normand: Consumers do not necessarily feel that they are in control, but equally I am not sure their being in control is necessarily feasible. What we have heard from consumers is how resigned and powerless they feel. The best example of that is the reaction to Cambridge Analytica, for example, where we heard that 24% of people said that as a result of that they would consider leaving Facebook and 6% did, and then actually the number of people logging on to Facebook went up.

The control bit may not be realistic. What we think people want is to know that there are controls, and they want to know that the system that they are operating in is not a wild west, that there is some degree of governance. They may not put it in terms of governance, but they want to know what would happen when something goes wrong. They want to know that there are rules around where their data goes. They want to understand how their data has been used, and to see how it has been used, and as a result of seeing that they can be more confident that it is not being used for nefarious or harmful purposes.

For us, that question of control is not so much putting people in the driving seat, with all of the responsibility that that creates, because that may not be what they really want. They want to know that they have a system they can trust in, that they can have confidence in, where they know that there are rules, that they can do something about the rules and that they have somewhere to go when things go wrong.

Baroness Chisholm of Owlpen: Should we go back to the beginning, so that there is transparency at the beginning when they first sign up to the data, so they know what the purpose of that data is? Do you think that would help?

Caroline Normand: Up to a point, through GDPR, we already have the requirement for people to understand what their data is being used for. That is a good step in the right direction, but it does not give them the specificity that allows them to understand later on, when they have probably forgotten what they signed up to, why they are seeing what they are seeing. It does not give them answers. Consumers as a whole think when they provide data that they are providing it into a bounded world. They do not really think that they are giving it into a world where data flows. They are finding that out and are then not able to find an answer saying, “It is okay because we have rules around where your data flows”. We cannot say that, because there are not. That sense of a system that has a degree of control about it is what is key here.

The Chairman: Thank you very much indeed for your evidence. Just to reiterate the point that Lady Quin made, could you write to us on matters to do with your international connections and the effect that Brexit may have on those networks?

There was just one other thing, which arises out of the question that you have just been answering, which is on the slightly narrower point of people’s awareness of their rights under existing data protection law. If you have anything that you could say to us about what assessment you have made of whether people are aware of their rights, and how willing or otherwise they are to exercise them, that would be very helpful.

In the meantime, thank you very much, again, for your evidence. I am sorry that it has felt a little pressured at the end, but you have been most helpful and we are very grateful. Thank you.

Caroline Normand, Director of Policy, Which? – supplementary written evidence (IRN0123)

At the oral evidence session on 24 October I promised to write to the Committee with further information in a number of areas of interest.

Action Fraud

The Committee asked us to provide further information regarding our research that estimated that less than more than 96% of frauds reported to Action Fraud are not solved (where solved means a suspect is charged, cautioned or receives an out-of-court penalty). Our estimate is derived from figures given to the Home Affairs Select Committee in a submission from the City of London Police in January 2018. Both Action Fraud and the National Fraud Intelligence Bureau (NFIB) are branches of the City of London Police. It is the NFIB which pools connected cases and considers whether there is a viable line of enquiry. If there is, it forwards the investigation to another agency which in most cases is a local police force, typically the one where the suspect resides.

Which? sent Freedom of Information requests to all 43 territorial police forces in summer 2018 asking them to provide the outcomes of fraud investigations for each of the past four years. More than two thirds of them responded. Although the data received from different forces does not enable us to directly compare the performance of difference forces, the figures clearly show a declining performance across the country. With the exception of Derbyshire every police force which released figures showed it had solved proportionally fewer fraud cases launched in 2016 than in 2014. Nearly all of them saw performance fall by more than 20% in the same period while 10 forces saw their solved rate fall by more than 40%. Overall the local police statistics still look healthier than the Action Fraud figures because the data from local forces only includes crimes passed on to them by NFIB and which have therefore been deemed to have a viable line of enquiry, as well as cases reported directly to the local police force.

Our work suggests several reasons for the poor resolution rate of fraud cases:

- Fraud is difficult to investigate because offenders are often 'invisible'. The Office for National Statistics estimates that around 55% of frauds have a digital element. Even with cutting-edge technologies to track down online or telephone fraudsters, investigators have an uphill battle compared with detectives working on a physical crime where there is CCTV evidence, eyewitness sightings etc.

- Police forces must prioritise and must weigh fraud cases against the threat, risk and harm of other offences, including violent crime.

- There is often a long delay between a case being reported to Action Fraud and it being referred on to a local police force – sometimes as long as five to six weeks. The NFIB have told us that the reasons for this include Data Protection Act requests to banks which can take weeks as the banks need to make checks before releasing the data; assessing other reports which may be linked; and the volume of reports that Action Fraud receives.

- Local forces sometimes refer fraud victims to Action Fraud when in fact the victim has information which, if acted upon quickly, might result in a suspect being apprehended. By the time the case is referred back from Action Fraud several weeks later that window of opportunity may be lost.

The City of London Police stressed to us that their fraud work goes beyond catching criminals and includes disrupting websites, telephone numbers and bank accounts linked to fraud. The detectives we interviewed from the City of London Police and from Manchester Police also stressed the increasing role that local police forces play in victim care, whether or not a case is being prosecuted.

I attach a copy of an article that appeared in the October edition of Which? Money, that contains further details.

Removal of unsafe products by online retailers and fake reviews

Baroness Quin asked us to provide details of how long it took for companies like Amazon and other online retailers to remove products from sale after Which? raised our concerns with them.

Our experience to date is that online retailers have responded promptly once the issue is raised with them, and that the products are typically removed within a couple of days. Of course our underlying concern is that there are unsafe products on sale in the first place and that unless an organisation like Which? is carrying out our own testing, then consumers are being exposed to dangerous goods. We therefore believe that the Government should consider what more online platforms could be doing to prevent potentially unsafe products from being sold to consumers.

In addition, last month we published the findings of an investigation we carried out into how fake reviews are being used by unscrupulous third-party sellers through legitimate retailers such as Amazon.

Customer reviews can be invaluable in helping us to choose what to buy. In our survey of more than 2,000 UK adults, 97% told us they use online customer reviews when researching a product. Fake reviews can artificially inflate ratings and rankings (where products appear in searches), and can result in customers being misled into buying poor-quality products based on customer review scores. The Competition and Markets Authority (CMA) estimates that £23bn a year of UK consumer spending is influenced by online customer reviews. But our research shows that fake reviews can have a detrimental effect on consumers.

We found that a network of Facebook groups had been set up to encourage purchasers to post favourable (four or five star) reviews on Amazon’s website in return for the reimbursement of their purchases. When we posed as a customer and posted an “honest” (one or two star) review, the sellers refused to reimburse our purchasers.

The effect of the United Kingdom leaving the European Union on the regulation of the internet

The Committee asked us what effect we anticipated the United Kingdom leaving the European Union will have on the regulation of the internet? We welcome the UK's continued implementation of the GDPR. Post exit, there should be an emphasis placed on continued cooperation around data protection to enable trade with the EU. Further to this, data protection must also be a priority as part of any future trade agreements that the UK seeks.

Domestically, organisations like the CMA/ICO will require additional resource to tackle large and complex digital and regulatory cases post the UK's exit from the EU.

A key consideration regarding the internet post exit also has to be the impact of no deal on consumer rights when shopping online from the EU. Reciprocal arrangements for enforcement and market surveillance between the UK and public authorities in EU countries would immediately end in the event of a no deal.

As such it will be harder for consumer to get refunds for good bought online from a company originating in an EU country that were faulty or did not fit with the way that they had been described. Consumers would have to take these up with the authorities in the country the business was based in.

Baroness Quin also asked us to set out how we envisage working with other consumer organisations post-Brexit. Which? is currently the largest member of the European Consumer Organisation, BEUC. Following a consultation with its members, BEUC's statutes are currently being revised so as to enable Which? to remain a fully participating member with the same rights and responsibilities as it currently has.

BEUC will remain an important information sharing hub for Which?, and will play an important role in helping to shape any future EU legislation which impacts UK consumers.

In conclusion, Which? is grateful that the Committee is examining these important issues, and we hope the Government, regulators and industry will take the Committee’s recommendations seriously.

Caroline Normand, Director of Policy, Which? – supplementary written evidence (IRN0123)

In particular we believe that there are four areas of work where action is required. Firstly, there needs to be greater focus by Government and regulators on understanding the impacts of consumer data use on individuals through the work of the new Centre for Data Ethics and Innovation. This should include providing consumers and their advocates with more transparency about the impact that personal data has on their lives. Secondly, the Centre for Data Ethics and Innovation should review the governance of data in motion, with due attention given to creative ways to improve oversight and enforcement. Thirdly, consumers need help understanding how to obtain redress in the event of a data breach. This may include the suitability of existing avenues of redress and how well informed consumers are about them. Finally, The Competition and Markets Authority (CMA) should conduct a market study in to the digital advertising industry as a matter of urgency.

5 November 2018

Robert White – written evidence (IRN0012)

Just because I am seventy-three years old I seem to become bombarded by adverts targeting me. Sometime ago I had a friend come to stay with a young baby. While shopping I agreed to get my friend some nappies. Over the next few days I was bombarded with adverts for nappies. I have to conclude that my credit card or store card must have passed on my details to third parties.
Since that episode I have become more conscious of being targeted especially by the hype for Bitcoins (and in particular so called Initial Coin Offerings or ICOs which are deliberate attempts to raise cash against worthless promises totally unconnected to Bitcoins themselves).

I have tried explaining the system of swindle to the Advertising Standards Agency (ASA) who replied with a totally weak solution and no help. Please see their answer included here [not attached].

The supposed reasoning is that the "fake news" and the actual scam cover several different stages of enticement and then claim individually each step to be innocent and unconnected.

I firmly believe that the responsibility for protecting the public lies with the social media companies obtaining revenue from what are called "Clickbait" diversions to "fake news" sites; while the social media companies in no way check where the diversion hyperlink is going to.

The companies I refer to are Google, Yahoo, Facebook, Twitter and Quora (there are probably many others that I, personally, don't use). The following pages demonstrate my actual experience [not attached].

7 May 2018

***Wired UK*, The *Guardian* and The *Times* – oral evidence (QQ 152-160)**

Transcript to be found under The *Guardian*

Professor Lorna Woods, Professor Christopher Marsden and Dr Victoria Nash – oral evidence (QQ 1-11)

Transcript to be found under Professor Christopher Marsden

Professor of Internet Law Lorna Woods, University of Essex and William Perrin – supplementary written evidence (IRN0047)

Professor Woods gave oral evidence on 24 April 2018 to the Lords Communications Committee Inquiry 'The Internet: to regulate or not to regulate?'. During the evidence session Professor Woods touched upon work she was doing with William Perrin and Carnegie UK Trust on designing a regulatory system to reduce harm on social media. The Chair asked Professor Woods for a note about this work which follows in the form of a summary and a full first draft of our work prepared for the Committee.

Summary

- Professor of Internet Law Lorna Woods and William Perrin have made a proposal to Carnegie UK Trust (Carnegie Proposal) for a regime to reduce harm from social media services as a sub-set of internet intermediaries.

- Social media service providers are not un-regulatable. We have faced far bigger and more profound issues before and have evolved a huge range of tools to correct corporate behaviours in the public interest. It has been policy since at least the 2000's, both at national and international level, that internet issues should be tackled wherever possible using 'physical world techniques' and social media is no exception.

- Social media service providers should each be seen as responsible for a public space, much as property owners or operators are in the physical world. In the physical world, Parliament has long imposed statutory duties of care upon property owners or occupiers in respect of people using their places, as well as on employers in respect of their employees. A duty of care is simple, broadly based and largely future-proof. It focusses on the objective and leaves the detail of the means to those best placed to come up with context-appropriate solutions – those who are subject to the duty of care. We suggest this model for the largest social media service providers – a duty of care in respect of their users, enforced in a risk-based manner by a regulator. The duty of care would not apply to online services with their own detailed rules such as the traditional media.

- A statutory duty of care to mitigate against certain harms be imposed on social media service providers with over 1,000,000 users/members/viewers in the UK in respect of their users/members. These categories of harm are to be specified in statute at a high level of generality. Those under a duty of care would be expected to identify the level of specified harms occurring through set-up and/or use of their respective platforms and take steps to reduce the level of harm, as set out below. This process would be monitored by an independent regulator. The regulator would be appointed and funded by a share of the revenue from the tax on internet company revenues that the government seems about to introduce.

- Central to the duty of care is the idea of risk. If a service provider targets or is used by a vulnerable group of users (e.g. children), its duty of care is greater and it should have more safeguard mechanisms in place than a service which is, for example, aimed at adults and has community rules agreed by the users themselves (not imposed as part of ToS by the provider) to allow robust or even aggressive communications.

- We envisage the harm reduction cycle to look something like this:

  - Each service provider works with the regulator, consulting civil society, to survey the extent and occurrence of harms, as set out by Parliament, in respect of the services provided by that provider;

  - Each service provider then produces and implements a plan to reduce the harms, having consulted the regulator and civil society;

  - Periodically, the harms are re-measured, the effectiveness of the plan assessed and, if necessary, further changes to company practices and to tools available to users introduced;

  - after a period the harms are measured again as above, new plans are produced and the cycle repeats;

  - progress towards harm reduction is monitored by the regulator, which may take regulatory action if progress is in the regulator’s view insufficient.

- Action that a provider could take is not just about take down notices but could include:

  - measures to empower users, for example pre-emptive blocking tools in the hands of the user; setting up sub-groups that have different toleration of certain types of language

  - effective complaints mechanisms both in respect of other users but also the company itself

  - transparency measures so that it is possible to see the number of complaints, the response, the mechanism by which the complaint was processed (human or automated) and the reasoning

  - review systems of company processes that assess them for nudging users to certain sorts of behaviours.

- The regulator would have the following responsibilities:

  - producing through a consultative process a list of the qualifying social service providers with more than 1,000,000 users/members etc in the UK. Being on or off that list is challengeable by judicial review.

  - monitoring the harm reduction processes run by the companies and supervises them into a continuous harm reduction cycle.
  - Providing advice as to scope of the harms, best practice on harm reduction;

  - enforcing the duty of care using tools such as enforcement notices, prohibition notices and fines.

- The list of qualifying social media service providers would likely include (but not necessarily be limited to):

  - Facebook
  - Twitter
  - YouTube
  - Instagram
  - Twitch
  - Snapchat
  - Musical.ly
  - Reddit
  - Pinterest
  - LinkedIn

- The regulator would have a range of sanctions from adverse behaviour notices though to administrative fines on the scale of those found in the GDPR. Individuals may be able to bring court action but we emphasise that this should only be in respect of systemic failures and not as a substitute for a civil action in relation to specific items of content.

Notes on the summary

- In our opinion this is compatible with EU law, in particular the e-Commerce directive. The immunity provisions relate to liability for the content of others and do not absolve providers from any duties of care.

- The preventive element of duty of care will reduce the suffering of victims. It may also prevent behaviours reaching a criminal threshold.

- A risk-managed approach only targeting the largest providers preserves freedom of speech. We envisage that platforms may take different approaches, and that a market could arise in which platforms develop aimed at particular groups. Content or speech patterns that are not acceptable on one platform may find a home elsewhere.

- Harms represent external costs generated by the production of the social media service providers' products. The duty of care, by requiring action to prevent harms internalises these costs to provider. This makes the market function more efficiently for society on the polluter pays principle and ultimately drives a more effective market which also benefits providers.

About the authors

- William Perrin and Lorna Woods have vast experience in regulation and free speech issues. William has worked on technology policy since the 1990s, was a driving force behind the creation of OFCOM and worked on regulatory regimes in many economic and social sectors while working in the UK government's Cabinet Office. He ran a tech start up and is now a trustee of several charities. Lorna is Professor of Internet Law at University of Essex, an EU national expert on regulation in the TMT sector, and was a solicitor in private practice specialising in telecoms, media and technology law.

- William and Lorna approached Carnegie UK Trust in January 2018 with a proposal to undertake this work pro bono. Carnegie has a strong track record in public policy as well as technology expertise as part of its Digital Futures programme and wider work on national wellbeing. Carnegie has been publishing blog posts as drafts of a final report which will be published in the Summer.

- The views expressed here are of the authors and not any other body.

Professor of Internet Law Lorna Woods, University of Essex and William Perrin – supplementary written evidence (IRN0047)

A Proposal for Harm Reduction

Survey of regulatory regimes

Harms and market failure

- The Government's Internet Safety Strategy Green Paper detailed extensive harms with costs to society and individuals resulting from people's consumption of social media services. Social media services companies early stage growth models and service design decisions appear to have been predicated on such costs being external to their own production decision. Effective regulation would internalise these costs for the largest operators and lead to more efficient outcomes for society.

- There is a good case to make for market failure in social media services – at a basic level people do not comprehend the price they are paying to use a social media service – recent research by doteveryone[1221] revealed that 70% of people 'don't realise free apps make money from data', and 62% 'don't realise social media make money from data'. Without basic awareness of price and value amongst consumers it will be hard for a market to operate efficiently, if at all. It would be interesting to see a full analysis of market failure in the sector.

Relevant regimes

- Assuming that some sort of regulation (or self or co regulation) is necessary to reduce harm, what form should it take? We surveyed regulatory regimes for communications, the digital economy, health and safety and the environment.[1222]

- There are many similarities between the regimes we surveyed. One key element of many of the regulators' approach is that changes in policy take place in a transparent manner and after consultation with a range of stakeholders. Further, all have some form of oversight and enforcement – including criminal penalties- and the regulators responsible are independent from both Parliament and industry. Breach of statutory duty may also lead to civil action. These matters of standards and of redress are not left purely to the industry.

[1221] Miller C, Coldicutt R and Kitcher H. (2018) People, Power and Technology: The 2018 Digital Understanding Report. London: Doteveryone, available: http://understanding.doteveryone.org.uk/files/Doteveryone_PeoplePowerTechDigitalUnderstanding2018.pdf

[1222] For more detail see 'Harm reduction in social media – what can we learn from other models of regulation?' May 4 2018 - https://www.carnegieuktrust.org.uk/blog/harm-reduction-social-media-can-learn-models-regulation/

- While the telecommunications model may seem an appropriate model give the telecommunications sector's closeness to social media, it may be that it is not the most appropriate model for four reasons:
    - the telecommunications regime gives the regulator the power of stopping the operator from providing the service itself, and not just problematic elements in relation to the service - we question whether this is appropriate in the light of freedom of speech concerns;
    - the telecommunications regime specifies the conditions with which operators must comply, albeit at a level of some generality – we feel that this is too 'top-down' for a fast moving sector and that allowing operators to make their own assessment of how to tackle risks means that solutions may more easily keep up with change, as well as be appropriate to the service;
    - a risk-based approach could also allow the platforms to differentiate between different types of audience – and perhaps to compete on that basis; and
    - the telecommunications regime is specific to the telecommunications context, the data and workplace regimes are designed to cover the risk entailed from broader swathes of general activity.
- Although the models have points of commonality, particularly in the approach of setting high level goals and then relying on the operators to make their own decisions how best to achieve that - there are perhaps aspects from individual regimes that are worth highlighting:
    - the data protection and HSE regime highlight that there may be differing risks with two consequences;
    - that measures should be proportionate to those risks; and
    - that in areas of greater risk there may be greater oversight.
    - The telecoms regime emphasises the importance of transparent complaints mechanisms – this is against the operator (and not just other users);
    - the environmental regime introduces the ideas of prevention and prior mitigation, as well as the possibility for those under a duty to be liable for the activities of others (eg in the case of fly-tipping by a contractor); and
    - the Digital Economy Act has mechanisms in relation to effective sanctions when the operator may lie outside the UK's jurisdiction.

Duty of care

- The idea of a "duty of care" is straightforward in principle[1223]. A person (including companies) under a duty of care must take care in relation to a particular activity as it affects particular people or things. If that person does not take care and someone comes to harm as a result then there are legal consequences. A duty of care does not require a perfect record – the question is whether sufficient care has been taken. A duty of care can arise in common law (in the courts) or, as our discussion of regulatory models above shows, in statute (set out in a law). It is this latter statutory duty of care we envisage. For statutory duties of care, as we set out above, while the basic mechanism may be the same, the details in each statutory scheme may differ – for example the level of care to be exhibited, the types of harm to be avoided and the defences available in case of breach of duty.

Social media services are like public spaces

- Many commentators have sought an analogy for social media services as a guide for the best route to regulation. A common comparison is that social media services are "like a publisher". In our view the main analogy for social networks lies outside the digital realm. When considering harm reduction, social media networks should be seen as a public place – like an office, bar, or theme park. Hundreds of millions of people go to social networks owned by companies to do a vast range of different things. In our view, they should be protected from harm when they do so.

- The law has proven very good at this type of protection in the physical realm. Workspaces, public spaces, even houses, in the UK owned or supplied by companies have to be safe for the people who use them. The law imposes a "duty of care" on the owners of those spaces. The company must take reasonable measures to prevent harm. While the company has freedom to adopt its own approach, the issue of what is 'reasonable' is subject to the oversight of a regulator, with recourse to the courts in case of dispute. If harm does happen the victim may have rights of redress in addition to any enforcement action that a regulator may take action against the company. We emphasise that this should only be in respect of systemic failures and not as a substitute for a civil action in relation to specific items of content. By making companies invest in safety the market works better as the company bears the full costs of its actions, rather than getting an implicit subsidy when society bears the costs.

A broad, general almost future-proof approach to safety

- Duties of care are expressed in terms of what they want to achieve – a desired outcome (ie the prevention of harm) rather than necessarily regulating the steps – the process – of how to get there. This fact means that duties of care

[1223] For more detail see 'Reducing harm in social media through a duty of care' May 8, 2018 https://www.carnegieuktrust.org.uk/blog/reducing-harm-social-media-duty-care/

work in circumstances where so many different things happen that you couldn't write rules for each one. This generality works well in multifunctional places like houses, parks, grounds, pubs, clubs, cafes, offices and has the added benefit of being to a large extent future-proof. Duties of care set out in law 40 years ago or more still work well – for instance the duty of care from employers to employees in the Health and Safety at Work Act 1974 still performs well, despite today's workplaces being profoundly different from 1974's.

- In our view the generality and simplicity of a duty of care works well for the breadth, complexity and rapid development of social media services, where writing detailed rules in law is impossible. By taking a similar approach to corporate owned public spaces, workplaces, products etc in the physical world, harm can be reduced in social networks. Making owners and operators of the largest social media services responsible for the costs and actions of harm reduction will also make markets work better.

Key harms to prevent

- When Parliament set out a duty of care it often sets down in the law a series of prominent harms, as can be seen in the 1974 Act, or areas that cause harm that Parliament feels need a particular focus, as a subset of the broad duty of care. This approach has the benefit of guiding companies on where to focus and makes sure that Parliament's priorities are not lost.

- We propose setting out the key harms that qualifying companies have to consider under the duty of care, based in part on the UK Government's Internet Safety Green Paper. We list here some areas that are already a criminal offence –the duty of care aims to prevent an offence happening and so requires social media service providers to take action before activity reaches the level at which it would become an offence.

  - Harmful threats – statement of an intention to cause pain, injury, damage or other hostile action such as intimidation. Psychological harassment, threats of a sexual nature, threats to kill, racial or religious threats known as hate crime. Hostility or prejudice based on a person's race, religion, sexual orientation, disability or transgender identity. We would extend the understanding of "hate" to include misogyny.

  - Economic harm – financial misconduct, intellectual property abuse,

  - Harms to national security – violent extremism, terrorism, state sponsored cyber warfare

  - Emotional harm – preventing emotional harm suffered by users such that it does not build up to the criminal threshold of a recognised psychiatric injury. For instance through aggregated abuse of one person by many others in a way that would not happen in the physical world (see

Stannard[1224] on emotional harm below a criminal threshold). This includes harm to vulnerable people – in respect of suicide, anorexia, mental illness etc.

- Harm to young people – bullying, aggression, hate, sexual harassment and communications, exposure to harmful or disturbing content, grooming, child abuse (See UKCCIS Literature Review[1225])

- Harms to justice and democracy – prevent intimidation of people taking part in the political process beyond robust debate, protecting the criminal and trial process (see concerns expressed by the Attorney General[1226] and the Committee on Standards in Public Life[1227])

- We would also require qualifying social media service providers to ensure that their service was designed in such a way to be safe to use, including at a system design level. This represents a hedge against unforeseen developments as well as being an aggregate of preventing the above harms. We have borrowed this idea from risk based regulation in the General Data Protection Regulation and the Health and Safety at Work Act which both in different ways require activity to be safe or low risk by design[1228].

- People would have rights to sue eligible social media service providers under the duty of care; for the avoidance of doubt, a successful claim would have to show a systemic failing rather than be deployed in case of an isolated instance of content. But, given the huge power of most social media service companies relative to an individual we would also appoint a regulator. The regulator would ensure that companies have measurable, transparent, effective processes in place to reduce harm, so as to help avoid the need for individuals to take action in the first place. The regulator would have powers of sanction if they did not.

Which social media services would be subject to a statutory duty of care towards their users?

[1224] J E Stannard, 'Sticks, Stones and Words: Emotional Harm and the English Criminal Law' (2010) 74 *Journal of Criminal Law* 533, available: http://journals.sagepub.com/doi/abs/10.1350/jcla.2010.74.6.668

[1225] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/650933/Literature_Review_Final_October_2017.pdf

[1226] Attorney General The Impact of Social Media on the Administration of Justice: call for evidence, 15 September 2017, available: https://www.gov.uk/government/publications/the-impact-of-social-media-on-the-administration-of-justice

[1227] See Committee on Standards in Public Life Intimidation in Public Life, A Review by the Committee on Standards in Public Life, December 2017, Cm 9543, available: https://www.gov.uk/government/publications/intimidation-in-public-life-a-review-by-the-committee-on-standards-in-public-life

[1228] The Network and Information Systems Regulations 2018 have a similar risk based approach http://www.legislation.gov.uk/uksi/2018/506/contents/made. On this generally, see https://www.carnegieuktrust.org.uk/blog/harm-reduction-social-media-can-learn-models-regulation/

- Parliament would set out in law characteristics of social media services that could be covered by the regime. There are always difficult boundary cases and to mitigate this we propose the regulator makes a list of qualifying services[1229].

Qualifying social media services

- We suggest that the regime apply to social media services used in the UK that have the following characteristics:
  - Have a strong two-way or multiway communications component;
  - Display and organise user generated content publicly or to a large member/user audience;
  - A significant number of users or audience – more than, say, 1,000,000;
  - Are not subject to a detailed existing regulatory regime, such as the traditional media.
- A regulator would produce detailed criteria for qualifying social media services based on the above and consult on them publicly. The regulator would be required to maintain a market intelligence function to inform consideration of these criteria. Evidence to inform judgements could come from: individual users, civil society bodies acting on behalf of individuals, whistle-blowers, researchers, journalists, consumer groups, the companies themselves, overseas markets in which the services operate, as well as observation of trends on the platforms.
- In order to maintain an up to date list, **companies which fall within the definition of a qualifying social media service provider would be required in law to notify the regulator after they have been operating for a given period.** Failure to do so would be an offence – as it is a number of existing regulatory regimes. Notification would be a mitigating factor should the regulator need to administer sanctions.
- **The regulator will publish a list based on the notifications and on market intelligence, including the views of the public.** The regulator's decision to include a service on the list could, as for any such type of decision, be subject to judicial review, as could the decision not to include a service that the public had petitioned for. Services could be added to the list with due process at any time, but the regulator should review the entire list periodically, perhaps every two years.

[1229] Which social media services should be regulated for harm reduction? May 8, 2018 https://www.carnegieuktrust.org.uk/blog/social-media-services-regulated-harm-reduction/

- Broadly speaking we would anticipate at least the following social media service providers qualifying, we have asterisked cases for discussion below.

  - Facebook
  - Twitter
  - YouTube
  - Instagram
  - Twitch*
  - Snapchat
  - Musical.ly*
  - Reddit
  - Pinterest*
  - LinkedIn

Managing boundary cases

- **Providing a future proof definition of a qualifying social media service is tricky** However we feel that giving the independent regulator the responsibility to draw up a list allows for some future-proofing rather than writing it in legislation. The fact that it is the regulator which makes this list by reference to objective criteria also reduces the risk of political interference. It is quite proper for the government to act to reduce harm, but in our view there would be free speech concerns were the government to say who was on the list. An alternative would be for the regulator to advise the Secretary of State and for them to seek a negative resolution in Parliament but in our view this brings in a risk to independence and freedom of speech.

- Internet forums have some of the characteristics we set out above. However hardly any I forums would currently have enough members to qualify. The very few forums that do have over one million members have, in our opinion, reached that membership level through responsible moderation and community management. In a risk based regime (see below) they would be deemed very low risk and would be unlikely to have to change their processes significantly. We do not intend to capture blog publishing services, in our view the conversational interaction about a single blog, let alone a whole blogging service, is not on the scale of a social media service and they would not qualify.

- Twitch has well-documented abuse problems[1230] and has arguably more sophisticated banning regimes[1231] for bad behaviour than other social networks. Twitch allows gamers to stream content that the gamers have generated (on games sites) with the intention of interacting with an audience about that content. Twitch provides a place for that display, multiway discussion about it and provides a form of organisation that allows a user to find the particular content they wish to engage with. We therefore feel that Twitch falls within scope. Other gaming services with a strong social media element should also be considered, particularly with a strong youth user base.

- Note that services do not need to include (much) text or voice: photo sharing services such as Pinterest could fall within the regime too.

Risk based regulation – not treating all qualifying services the same

- This regime is risk based. We are not proposing that a uniform set of rules apply across very different services and user bases. The regulator would prioritise high risk services, and only have minimal engagement with low risk services. Differentiation between high and low risk services is common in other regulatory regimes, such as for data in the GDPR and is central to health and safety regulation. In those regimes, high risk services would be subject to closer oversight and tighter rules as we intend here.

- Harmful behaviours and risk have to be seen in the context of the platform. The regulator would examine whether a social media service operator has had particular regard to its audience. For example, a mass membership, general purpose service should manage risk by setting a very low tolerance for harmful behaviour, in the same way that some public spaces take into account that they should be a reasonably safe space for all. Specialist audiences/user-bases of social, media services may have online behavioural norms that on a family-friendly service could cause harm but in the community where they originate are not harmful. Examples might include sports-team fan services or sexuality-based communities. This can be seen particularly well with Reddit: its user base with diverse interests self organises into separate subreddits, each with its own behavioural culture and moderation.

- Services targeted at youths are innately higher risk – particularly where youth services are designed to be used on a mobile device away from immediate adult supervision. For example, teen focussed lip synching and video sharing site musical.ly owned by Chinese group Bytedance according to Channel 4 News[1232] has 2.5 million UK members and convincing reports of harmful

[1230] See e.g. Steffan Powell, "Twitch and YouTube 'taking misogynistic abuse in gaming seriously'" BBC Newsbeat, 28 Sept 2016, available: http://www.bbc.co.uk/newsbeat/article/37485834/twitch-and-youtube-taking-misogynistic-abuse-in-gaming-seriously

[1231] Twitch Community Guidelines Update, available: https://blog.twitch.tv/twitch-community-guidelines-updates-f2e82d87ae58?sf181649550=1

[1232] F Manji, 'Children bombarded with sexually explicit chat on Musical.ly and Live.ly' 8 Jun 2017, available: https://www.channel4.com/news/children-bombarded-with-sexually-explicit-chat-on-musical-ly-and-live-ly behaviours. The service is a phone app targeted at young people that also allows them to video cast their life (through their live.ly service) with as far as we can make out few meaningful parental controls. In our opinion, this appears to be a high risk service.

Regulation and enforcement

- Legislation should set the framework within which the regulator will act, allowing it some flexibility and to respond appropriately in a fast moving environment. Our proposal is that the regulator is tasked with ensuring that social media services providers have adequate systems in place to reduce harm. The regulator would not get involved in individual items of speech. The regulator must not be a censor.[1233]

Harm reduction cycle

- We envisage an ongoing evidence based process of harm reduction. For harm reduction in social media the regulator would work with the industry to create an on-going harm reduction cycle that is transparent, proportionate, measurable and risk-based.

- A harm reduction cycle begins with measurement of harms. The regulator would draw up a template for measuring harms, covering scope, quantity and impact. The regulator would use as a minimum the harms set out in statute but, where appropriate, include other harms revealed by research, advocacy from civil society, the qualifying social media service providers etc. The regulator would then consult publicly on this template, specifically including the qualifying social media service providers. Regulators in the UK such as the BBFC, the ASA and OFCOM (and its predecessors) have demonstrated for decades that it is possible to combine quantitative and qualitative analysis of media, neutral of political influence, for regulatory process.

- The qualifying social media services would then run a measurement of harm based on that template, making reasonable adjustments to adapt it to the circumstances of each service. The regulator would have powers in law to require the qualifying companies (see enforcement below) to comply. The companies would be required to publish the survey results in a timely manner. This would establish a first baseline of harm.

- The companies would then be required to act to reduce these harms. We expect those actions to be in two groups – things companies just do or stop doing, immediately; and actions that would take more time (for instance new code or terms and conditions changes). Companies should seek views from

[1233] For more detail see 'How would a social media harm regulator work?' May 10, 2018 https://www.carnegieuktrust.org.uk/blog/social-media-harm-regulator-work/

users as the victims of harms or NGOs that speak for them. These comments – or more specifically the qualifying social media service providers respective responses to them (though it should be emphasised that companies need not adopt every such suggestion made) – would form part of any assessment of whether an operator was taking reasonable steps and satisfying its duty of care. Companies would be required to publish, in a format set out by the regulator:

  - what actions they have taken immediately;
  - actions they plan to take;
  - an estimated timescale for measurable effect; and
  - basic forecasts for the impact on the harms revealed in the baseline survey and any others they have identified.

- The regulator would invite views on the plan from the public, industry, consumers/users and civil society and make comments on the plan to the company, including comments as to whether the plan was sufficient and/or appropriate. The companies would then continue or begin their harm reduction work based on their individual plans.
- Harms would be measured again after a sufficient time has passed for harm reduction measures to have taken effect, repeating the initial process. This establishes the first progress baseline.
- The baseline will reveal four likely outcomes – that harms:
  - have risen;
  - stayed the same;
  - have fallen; or
  - new harms have occurred.
- If harms surveyed in the baseline have risen or stayed the same the companies concerned will be required to act and plan again, taking due account of the views of victims, NGOS and the regulator. In these instances, the regulator may take the view that the duty of care is not being satisfied and, ultimately, may take enforcement action (see below). If harms have fallen then companies will reinforce this positive downward trajectory in a new plan. Companies would prepare second harm reduction reports/plans as in the previous round but including learning from the first wave of actions, successful and unsuccessful. Companies would then implement the plans. The regulator would set an interval before the next wave of evaluation and reporting.

- Well-run social media services would quickly settle down to much lower level of harm and shift to less risky designs. This cycle of harm measurement and reduction would continue to be repeated, as in any risk management process participants would have to maintain constant vigilance.

- At this point we need to consider the impact of the e-Commerce Directive which gives immunity from liability to neutral intermediaries under certain conditions. Although we are not convinced that all qualifying social media companies would be neutral intermediaries within the meaning of the directive, there is a question as whether some of the measures that might be taken as part of a harm reduction plan could mean that the qualifying company which was neutral would lose its immunity, which would be undesirable. There are three comments that should be made here to mitigate this concern:

  - Not all measures that could be taken would have this effect;

  - The Commission has suggested that the e-Commerce Directive be interpreted – in the context of taking down hate speech and other similarly harmful content[1234] as not meaning that those which take proactive steps to prevent such content should be regarded as thereby assuming liability;

  - After Brexit, there may be some scope for changing the immunity regime – including the chance to include a 'good Samaritan defence' expressly.

- This harm reduction cycle is similar to the techniques used by the Commission in a series of documents as it works with the social media service providers to remove violent extremist content.[1235]

Other regulatory techniques

- Alongside the harm reduction cycle we would expect the regulator to employ a range of techniques derived from harm reduction practice in other areas of regulation. We draw the following from a wide range of regulatory practice rather than the narrow set of tools currently employed by the tech industry (take down, filtering etc). Some of these the regulator would do, others the regulator would require the companies to do.

- For example, each qualifying social media service provider could be required to:

[1234] Commission Recommendation on measures to effectively tackle illegal content online (C(2018) 1177 final) 1 March 2018, available: https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online

[1235] See e.g. Commission Recommendation (n 14) and Communication Tackling Illegal Content Online (COM (2017) 555 final), available: https://ec.europa.eu/digital-single-market/en/news/communication-tackling-illegal-content-online-towards-enhanced-responsibility-online-platforms

  - develop a statement of risks of harm, prominently displayed to all users when the regime is introduced and thereafter to new users; and when launching new services or features;

  - provide its child protection and parental control approach, including age verification, for the regulator's approval;

  - display a rating of harm agreed with the regulator on the most prominent screen seen by users;

  - work with the regulator and civil society on model standards of care in high risk areas such as suicide, self-harm, anorexia, hate crime etc; and

  - provide adequate complaints handling systems with independently assessed customer satisfaction targets and also produce a twice yearly report on the breakdown of complaints (subject, satisfaction, numbers, handled by humans, handled in automated method etc.) to a standard set by the regulator.

- The regulator would:

  - publish model policies on user sanctions for harmful behaviour, sharing research from the companies and independent research;
  - set standards for and monitoring response time to queries (as the European Commission does on extremist content through mystery shopping);

  - co-ordinate with the qualifying companies on training and awareness for the companies' staff on harms;

  - contact social media service companies that do not qualify for this regime to see if regulated problems move elsewhere and to spread good practice on harm reduction

  - publish a forward-look at non-qualifying social media services brought to the regulator's attention that might qualify in future;

  - support research into online harms – both funding its own research and co-ordinating work of others;

  - establish a reference/advisory panel to provide external advice to the regulator – the panel might comprise civil society groups, people who have been victims of harm, free speech groups; and

  - maintain an independent appeals panel.

Consumer redress

- We note the many complaints from individuals that social media services companies do not deal well with complaints. The most recent high profile example is martin Lewis's case against Facebook.[1236] At the very least qualifying companies should have internal mechanisms for redress that meet standards set by an outside body of simplicity (as few steps as possible), are fast, clear and transparent. We would establish, or legislate to make the service providers do so, a body or mechanism to improve handling of individual complaints. There are a number of routes which require further consideration – one route might be an ombudsman service, commonly used with utility companies although not with great citizen satisfaction, another might be a binding arbitration process or possibly both.

- Publishing performance data (specifically in relation to complaints handling) to a regulatory standard would reveal how well the services are working. We wish to ensure that the right of an individual to go to court is not diluted, which makes the duty of care more effective, but recognise that that is unaffordable for many. None of the above would remove an individual's right to go to court, or to the police if they felt a crime had been committed.

Sanctions and compliance

- Some of the qualifying social media services will be amongst the world's biggest companies. In our view the companies will want to take part in an effective harm reduction regime and comply with the law. The companies' duty is to their shareholders – in many ways they require regulation to make serious adjustments to their business for the benefit of wider society. The scale at which these companies operate means that a proportionate sanctions regime is required. We bear in mind the Legal Services Board paper on Regulatory Sanctions and Appeals processes:

  'if a regulator has insufficient powers and sanctions it is unlikely to incentivise behavioural change in those who are tempted to breach regulators requirements.'[1237]

- Throughout discussion of sanctions there is a tension with freedom of speech. The companies are substantial vectors for free speech, although by no means exclusive ones. The state and its actors must take great care not to be seen to be penalising free speech unless the action of that speech infringes the rights of others not to be harmed or to speak themselves. The sanctions regime should penalise bad processes or systems that lead to harm.

[1236] M. Lewis, 'Martin Lewis: Suing Facebook left me shaking - it's now admitted 1,000s of fake ads, here's the latest', 1st May 2018 updated 2nd May 2018, available: https://blog.moneysavingexpert.com/2018/05/martin-lewis--suing-facebook--left-me-shaking--it-s-now-admitted/

[1237] Legal Services Board, Overseeing Regulation: The LSB's Approach to Its Role, June 2013, available: http://www.legalservicesboard.org.uk/news_publications/LSB_news/PDF/2013/20130611_LSB_Sets_Out_Its_Approach_To_Overseeing_Regulation.pdf

- All processes leading to the imposition of sanctions should be transparent and subject to a civil standard of proof. By targeting the largest companies, all of which are equipped to code and recode their platforms at some speed, we do not feel that the argument that 'the problem is too big' is adequate. There may however be a case for some statutory defences.

- Sanctions would include:

  - Administrative fines in line with the parameters established through the Data Protection Bill regime of up to €20 million, or 4% annual global turnover – whichever is higher.

  - Enforcement notices – (as used in data protection, health and safety) – in extreme circumstances a notice to a company to stop it doing something. Breach of an enforcement service could lead to substantial fines.

  - Enforceable undertakings where the companies agree to do something to reduce harm.

  - Adverse publicity orders – the company is required to display a message on its screen most visible to all users detailing its offence. A study on the impact of reputational damage for financial services companies that commit offences in the UK found it to be nine times the impact of the fine.[1238]

  - Forms of restorative justice – where victims sit down with company directors and tell their stories face to face.

Sanctions for exceptional harm

- The scale at which some of the qualifying social media services operate is such that there is the potential for exceptional harm. It is not impossible to imagine a social media service being exploited to provoke a riot. Imagine people were severely injured or died and widespread economic damage was caused as a result. The regulator had warned about harmful design features in the service, those flaws had gone uncorrected, the instigators or the spreaders of insurrection exploited deliberately or accidentally those features. Or sexual harm occurs to hundreds of young people due to the repeated failure of a social media company to provide parental controls or age verification in a teen video service. Are fines enough or are more severe sanctions involving the criminal required, as seen elsewhere in regulatory schemes?

[1238] Armour et al, 'Regulatory Sanctions and Reputational Damage in Financial Markets' (2017) 52 Journal of Financial and Quantitative Analysis 1429-1448, available: https://www.cambridge.org/core/journals/journal-of-financial-and-quantitative-analysis/article/regulatory-sanctions-and-reputational-damage-in-financial-markets/462D1A709D61F3B94605A64E626A3DEE

- In extreme cases should there be a power to send a social media services company director to prison or to turn off the service? Regulation of health and safety in the UK allows the regulator in extreme circumstances which often involve a death[1239] or repeated, persistent breaches[1240] to seek a custodial sentence for a director. The Digital Economy Act contains power (Section 23) for the age verification regulator to issue a notice to internet service providers to block a website in the UK. In the USA the new FOSTA-SESTA package apparently provides for criminal penalties (including we think arrest) for internet companies that facilitate sex trafficking. This led swiftly to closure of dating services and a sex worker forum having its DNS service withdrawn in its entirety.

- **None of these powers sit well with the protection of free speech on what are generalist platforms – withdrawing the whole service due to harmful behaviour in one corner of it deprives innocent users of their speech on the platform. However, the scale of social media service mean that acute large scale harm can arise that would be penalised with gaol elsewhere in society. Further debate on this aspect is needed.**

Who should regulate to reduce harm in social media services?

- We now address two linked questions:
    - why a regulator is necessary, as we have already implied it is; and
    - the nature of that regulator.[1241]

The Need for a Regulator

- The first question is whether a regulator is needed at all if a duty of care is to be created.

- Is the fact that individuals may seek redress in relation to this overarching duty (by contrast to an action in relation to an individual piece of content) in the courts not sufficient? At least two pieces of profound legislation based on duties of care do not have 'regulators' as such – the 1957 Occupiers Liability Act and the 1973 Defective Premises Act. By contrast, the 1974 Health and Safety at Work Act does rely on a regulator, now the Health and Safety Executive (HSE). A regulator can address asymmetries of power between the

[1239] e.g. L Applebey 'Site manager jailed following fatal fall' Health and Safety Practitioner, 19 July 2016, available: https://www.shponline.co.uk/site-manager-jailed-following-fatal-fall/

[1240] e.g. Health and Safety Executive, 'Four Receive Suspended jail Sentences for Health and Safety Failings', 16 November 2016, available: http://press.hse.gov.uk/2016/four-receive-suspended-jail-sentences-for-health-and-safety-failings/

[1241] See Who should regulate to reduce harm in social media services? May 10, 2018 https://www.carnegieuktrust.org.uk/blog/regulate-reduce-harm-social-media-services/

victim and the harm causer. It is conceivable for a home owner to sue a builder or a person for harm from a building, or a person to sue a local authority for harm at a playground. However there is a strong power imbalance between an employee and their boss or even between a trade union and a multinational. A fully functioning regulator compensates for these asymmetries. In our opinion there are profound asymmetries between a user of a social media service and the company that runs it, even where the user is a business, and so a regulator is required to compensate for the users' relative weakness.

What Sort of Regulator?

- Assuming a regulator is needed, should it be a new regulator from the ground up or an existing regulator upon which the powers and resources are conferred? Need it be a traditional regulator, or would a self or co-regulator suffice? We would not at this stage rule out a co-regulatory model, although our preliminary conclusion is that a regulator is required. As we shall see below, instances of co-regulation in the communications sector have run into problems. Self-regulation works best when the public interest to be served and those of the industry coincide. This is not the case here.

- Whichever model is adopted, the important point is that the regulator be independent (and its members comply with the Nolan Principles[1242]). The regulator must be independent not only from government but also from industry, so that it can make decisions based on objective evidence (and not under pressure from other interests) and be viewed as a credible regulator by the public. Independence means that it must have sufficient resources, as well as relevant expertise.

- A completely new regulator created by statute would take some years before it was operational. OFCOM, for instance, was first proposed in the Communications White Paper in December 2000, was created in a paving act of Parliament in 2002 but did not vest and become operational until December 29 2003 at a cost of £120m (2018 prices). In our view harm reduction requires more urgent (and less expensive) action.

- We therefore propose extending the competence of an existing regulator. This approach has a number of advantages. It spreads the regulator's overheads further, draws upon existing expertise within the regulator (both in terms of process and substantive knowledge) and allows a faster start. We consider that the following (co) regulators should be considered: Advertising Standards Authority (ASA), the British Board of Film Classification (BBFC), the Health and Safety Executive (HSE) or the Office of Communications (OFCOM), all of which have the long proven regulatory ability.

[1242] Committee on Standards in Public Life, The Seven Principles of Public Life, 31 May 1995, available: https://www.gov.uk/government/publications/the-7-principles-of-public-life

- The BBFC seems to have its hands full with the age verification regulator from the Digital Economy Act 2017. The launch date has been missed for reasons that are unclear and in our view this removes them from consideration. This also raises the question of how well delegated responsibilities work; Ofcom has recently absorbed responsibilities in relation to video on demand, rather than continue to delegate them to ATVOD. While the ASA regulates some content online including material on social media platforms, but this is limited to advertisements (including sponsorship and the like). Overall the ASA focusses quite tightly on advertising; this may test its expertise. Adding in the substantial task of grappling with harm social media services more broadly could damage its core functions. The HSE has a strong track record in running a risk based system to reduce harm in the workplace, including to some extent emotional harm[1243]. It has a substantial scientific and research capability, employing over 800 scientists and analysts. However our judgement is that harm reduction in social media service providers require a regulator with deep experience of and specialism in online industries, which is not where the HSE's strengths lie.

- Our recommendation is to vest the powers to reduce harm in social media services to OFCOM. OFCOM has over 15 years' experience of digital issues, including regulating harm and protecting young people in broadcasting, a strong research capability, proven independence, a consumer panel, and also resilience in dealing with multinational companies. OFCOM is of a size (£110-£120 annual income and 790 staff) where, with the correct funding it could support an additional organisational unit to take on this work without unbalancing the organisation.

- The regulator could be funded by a small fraction of the revenue planned to be raised by the Treasury from taxing the revenues of internet companies[1244], of which this would be but a tiny percentage. The relative costs of large regulators suggest that the required resource would be in the low tens of millions of pounds.

Simple legislation to pass quickly

- Action to reduce harm on social media is urgently needed. We think that there is a relatively quick route to implementation in law. A short bill before parliament would create a duty of care, appoint, fund and give instructions to a regulator.

- We have reviewed the very short Acts that set up far more profound duties of care than regulating social media services – The Defective Premises Act 1972

[1243] HSE, Work-related stress and how to tackle it, available: http://www.hse.gov.uk/stress/what-to-do.htm

[1244] K. Ahmed 'Tech giants face new UK tax clampdown' BBC News 22 February 2018, available: http://www.bbc.co.uk/news/business-43161736 is only seven sections and 28 clauses (very this was unusually a private members bill written by the Law Commission); the Occupiers Liability Act 1957 is slightly shorter. The central clauses of the Health and Safety at Work Act 1974 creating a duty of care and a duty to provide safe machines are brief.

- For social media services, a duty of care and key harms are simple to express in law, requiring less than ten clauses or less if the key harms are set out as sub clauses. A duty for safe design would require a couple of clauses. Some further clauses to amend the Communications Act 2003 would appoint OFCOM as the regulator and fund them for this new work. The most clauses might be required for definitions and parameters for the list the regulator has to prepare. We speculate that an overall length of six sections totalling thirty clauses might do it. This would be very small compared to the Communications Act 2003 of 411 Sections, thousands of clauses in the main body of the Act and 19 Schedules of further clauses.

- This makes for a short and simple bill in Parliament that could slot into the legislative timetable, even though it is crowded by Brexit legislation. If government did not bring legislation forward a Private Peers/Members Bill could be considered.

- We are considering drafting such a bill to inform debate and test our estimate.

11 May 2018

Yoti - written evidence (IRN0067)

Introduction

The British Government is working to establish the “world's more dynamic digital economy”, and want to ensure that it is the world’s safest as well.[1245] There is no doubt that the internet is a great contributor to society, however it has brought complex problems that put vulnerable people at risk.

Increasingly in the UK both politicians and industry influencers are saying that the internet should not be the Wild West and what is “unacceptable offline should be unacceptable online”.[1246] Yoti, a digital identity platform, shares these concerns and believes that regulations should be in place in order to guarantee safety to the population.

There is strong potential for technology innovation to assist those combating online crime and improving safety we would like to discuss the following areas, where we believe that digital identity can support the fight against online harms, violence and fraud:

- Online Safety
    - Age Appropriate Access to Content be that under 13, under 18 or over 18
    - Knowing who you are dealing with - online dating
    - Classified sites - verified seller profiles
    - Peer to Peer identity details swap
    - Polling - One person one vote
    - Safer Password Management

- Freedom of Expression
    - Pseudonymisation

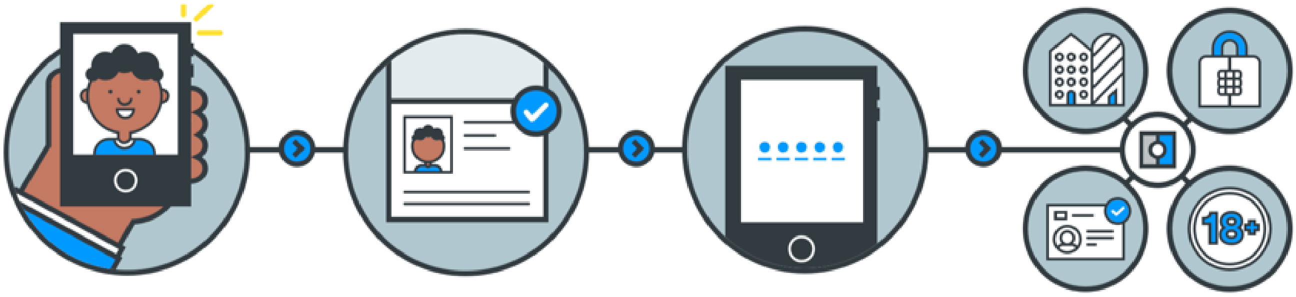
Yoti Background

Yoti is a UK founded and funded identity checking system that allows organisations to verify who people are, online and in person. It is a team of 250 based in London and Chelmsford, with offices in Mumbai and due to open offices in the US and Canada later in 2018. Yoti launched in November 2017 and so far over 1 million people have downloaded the app. Yoti has been announced as the eID provider for the States of Jersey and recently secured India's leading dating site as a verification partner and are

[1245] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf

[1246] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf

due to start working with the second largest peer to peer marketplace with 30m monthly users and one of India's biggest banks with 80m account holders..
For consumers, it’s an app that helps them prove who they are and confirm the identities of others. The company distinguishes itself with its approach to privacy and security - earning money from businesses when users voluntarily share verified attributes e.g. for KYC (see FAQs for technical detail). The app is available in the app stores and is free to download. The set-up involves a four-minute process, where you link your facial biometrics to your phone and verify your identity by scanning in a verified photo ID document. Identities are verified using NIST approved facial recognition technology, that matches individuals with their government issued identity documents and where possible, biometric passport chips. As well as using facial recognition technology a trained security team review the integrity of the documents and check the faces match. Once you've completed set-up, your Yoti securely holds verified attributes of your identity, such as name, date of birth, gender, nationality. You can then use the app to scan QR codes to pass specific attributes to other people or organisations or websites. This might be for age verification in the offline or online world or to populate verified data on an online form.



Add biometrics

User downloads app and creates a profile by taking a selfie and verifying their phone number.

Yoti's proprietary technology checks the user is a real person to ensure fake videos or photos aren't being used.

Adds government ID

User adds government issued passport or driving licence.

Yoti matches with biometrics and transforms information into a unique digital identity.

Encrypt data

User secures with a 5 digit PIN.

Yoti stores data with bank level encryption. Yoti cannot cannot access their data once the user's profile is verified.

Share details

Users connect and verify their details with a range of organisations using their Yoti everyday.

Yoti have been part of the UK Digital Policy Alliance steering group creating the 1296 Age Checking PAS, which is being made into a British Standards, chaired by Lord Erroll at Westminster ahead of the Digital Economy Act. Yoti serves as industry chair for the DPA Age Verification & Internet Safety Steering Group; is sponsor of the APPG Digital Identity and serves on the Home Office Identity Document Working Group and is a member of the newly formed Association of Document Validation Professionals. The Yoti team serve on several TechUK boards - for Justice & Emergency Services, Data Protection and Digital Identity. Yoti are a key partner of London Digital Security Centre, set up by City of London Police, Met Police and the London Mayor's Office to help businesses innovate, grow and prosper through operating in a secure digital environment and accredited by Met Police Secure by Design. Yoti are a registered BCorps and have set up a Guardians Council to hold them to account; as well as working with Responsible 100, Doteveryone Sustainable Tech Trust Mark Prototyping, EU Compass Responsible Innovation to assist in developing an ethics framework.

Digital identity can help to ensure online safety as well as the freedom of expression and information in the following ways:

1. Online Safety

Yoti is working in a number of ways to help young people stay safe online.

- Age Appropriate Access to Content be that under 13, under 18 or over 18

Adult Content

As young people's access to the internet increases, their risk to 'stumble upon' inappropriate content also increases. NSPCC ChildLine statistics reported that in the past three years over 2000 children have seen upsetting, pornographic content online.[1247] ChildLine also revealed that *"children as young as 11 are contacting ChildLine with concerns about porn"* and that children said that "*watching porn is making them feel depressed, giving them body image issues, making them feel pressured to engage in sexual acts they're not ready for and some even feel they are addicted to porn"*[1248]

Under the Digital Economy Act, if an adult wishes to access adult content they will be required to age verify. Via Yoti an adult can share anonymously an 'over 18 attribute' and verify with their biometrics that they are simply over the age of 18, thereby protecting children from accessing age inappropriate material.

Yoti verifies the user is genuine, but no other personal identity details are shared with the adult content provider, making it safer and more private than using a paper ID document, and limiting risk of personal identity exposure.

Neither Yoti nor the adult website accepting Yoti will have access to any information about the individual - except that they are over 18. Yoti is built with privacy by design:

- Yoti only keeps a copy of the ID document for up to 7 days after a user has registered while the account is proven genuine. The document image is then deleted.
- Once created ID details have been verified, Yoti does not see any personal details.
- Yoti doesn't see any of the information being shared between a business and customers, and can not track people's personal activity.

[For demonstration see https://yoti-online-age-check.herokuapp.com/]

[1247] http://www.dailymail.co.uk/news/article-5507751/NSPCC-offers-counselling-children-young-11- addicted-porn.html

[1248] http://www.childnet.com/blog/childline-fapz-campaign

The BBFC has shared its regulatory guidance for electronic age verification stating Name, DoB and Address entry will not alone be acceptable for proof of age when AV is required by adult content sites later in 2018. Hence it is important to be open to and understand innovations in digital identity.

Protecting Under 18s - A tool for Under 18s to report and remove

Yoti has partnered with NSPCC and the Internet Watch Foundation (IWF) to create a reporting tool which helps young people to flag and take down indecent images or videos of themselves online.

Yoti also provides a robust Age Verification (AV) system using biometrics which enables a child to share a anonymously an 'under 18 attribute' to apply to have an indecent image removed.

Age gating and Parental Consent

Likewise, Yoti can prevent adults from entering child content sites by enabling a site to request an 'under 18 attribute' or an 'under 13 attribute'. Current age verification methods are flawed - merely requiring a tickbox or simple 'double email' confirmation when it comes to parent consent, which can allow underage or allowing malicious people have access to content.

Yoti's biometric digital identity offers a robust way to verify the age of people entering platforms and to also have an audit trail of clear parental consent. Parental consent can also be revoked for a site.

We are observing that companies serving either the adult or child online content markets are now starting to explore technology innovations that can safeguard children and deliver more loyal customers. They also realise the high potential costs in financial, societal and public relations terms from not complying with GDPR or COPPA regulations.

- **Knowing who you are dealing with - online dating**

It today's world there are many circumstances when it is hard to know if you are dealing with the person that you think you are dealing with online and to be able to trust the counterparty. Online dating, classified and social networking sites are three examples where verified digital identities could help to rebuild trust.

Romance fraud scams are a growing issue for policing. In 2016 there were an estimated of 7.8 million people using online dating in the UK. A report by the

National Fraud Intelligence Bureau revealed that the losses reported due to dating fraud reached £39 million in 2014.[1249]

Creating a fake social media account and then using that to create a dating profile is very easy. It requires just an email address which can be created in seconds. MP Ann Coffey commented: *"Catfishing is a modern day menace affecting the lives of many innocent people. It can cause years of heartache. We must do something to deter this and a change in the law is the most effective deterrent."* Hence, Ann Coffey is lobbying for a new law to classify catfishing as an offence.[1250]

Conscious of how false identities can be misused on online dating platforms, Yoti is keen to support a safer dating environment by verifying the identity of the people who join these sites. Yoti has partnered with a leading online dating site in India, Truly Madly. People can use their Yoti to share a limited number of verified attributes, for example their name or gender, enabling users to increase their trust score on the site. Linking their profile to a Government issued identity document is a strong deterrent to fraud and crime and builds trust in the dating platform.

For more information see: https://www.yoti.com/blog/trulymadly-and-yoti-build-a-safer-community-of-online-daters/

- **Verified profiles for classified sites or online review sites**

Criminals are also targeting classified sites, using fake identities to offer goods and services and then blackmailing their victims to send money or sexual images. One such example was the Matthew Falder case, a paedophile who blackmailed at least 47 people to send humiliating pictures of themselves.[1251]

A way to prevent this is for the classified site to verify the identity of the users. Freeads for instance is a UK based site where sellers can be verified to their Yoti to achieve 'Trusted Seller Status' and government issued identity document.

Here is a short video of this.

Verified profiles could also enable a reviewer to be a verified reviewer linked to their Government issued identity document, to increase faith in online reviews.

- **Peer to Peer identity details swap**

One of the Yoti app's earliest functionalities is the peer to peer swap. The Yoti app is free for users to install and peer to peer swaps are also free. The simple act of swapping checked and verified identity details like name, date of birth

[1249] http://www.bbc.co.uk/news/uk-38678089
[1250] http://anncoffeymp.com/archives/243
[1251] http://www.dailymail.co.uk/news/article-5410677/Cambridge-graduates-life-online-paedophile.html

and say a verified photo, could help to reduce crime. Fraudsters typically do not like to reveal their identity, linked to a Government issued identity document, leaving an audit receipt trail behind them. For instance when buying a second hand good from someone, you may choose to swap just a photo and over 18 status to help to recognise the person when you meet up and to ensure that you are dealing with an adult. Ahead of a date, you may wish to exchange gender, photo and over 18 status.

- **Polling - One person one vote**

Another example where people also create fake accounts is for online polling or online voting. To make a survey poll or voting credible it is important to limit it to one vote per person; however, there are many cases where people use multiple accounts to manipulate results. Such is the case of the Brit awards this year, where a number of suspicious votes were detected through ‘fake’ Twitter accounts.[1252] Yoti’s digital identity enables people to vote anonymously so that organisers can be confident that behind each of the votes there is a legitimate person - not a bot - and they have only participated once.

See video: https://www.youtube.com/watch?v=fzlzxFZGWuQ

- **Safer Password Management**

Nowadays, online accounts cover many realms of daily life, from utility bills, to banking, to social networks and work email. The concept of individual identity has evolved and goes beyond a physical identity and now extends in the online world to usernames and passwords.

In 2016 alone, 3.3 bn login credentials were stolen. In the same year 9 out of 10 login attempts were fraudulent[1253]. Some of the causes of password theft are because passwords are weak, users re-use the same password for several accounts and users save their login details in an unsafe way.

Yoti offers a free Password Manager tool to solve this problem. It eliminates the need for users to remember passwords and generates strong passwords which are very hard for humans and computers to guess, plus it saves and retrieves passwords securely using military grade AES-256 encryption.

Yoti Password Manager provides a more robust way to manage passwords and crucially it doesn’t rely on master passwords. It combines verified digital identities with an individual’s unique biometric data to make the user the only person that can access their passwords, hence their accounts.

[1252] https://www.thetimes.co.uk/article/fake-twitter-voters-try-to-rig-brit-awards-mvkd9jq78

[1253] http://info.shapesecurity.com/2017-Credential-Spill-Report.html

To use Yoti Password Manager the person needs to download the free Yoti app and create a Yoti account, which takes only four minutes. Afterwards the user needs to install the free YPM extension for Chrome or Firefox on PC or Mac and then it is ready to use.

Set up a Yoti account:
https://www.youtube.com/watch?reload=9&v=mI_H8JfT2aU

Yoti Password Manager:
https://www.facebook.com/getYoti/videos/855743401299577/

2. Freedom of Expression

In order to protect both freedom of expression and freedom of information, a mechanism is needed to remove content online and to contest when content is requested to be removed. In both instances it is also necessary for the internet service provider to be able to identify the party requesting the content to be removed or reinstated.

The ability to identify the party requesting for content to be removed is crucial in order to prevent abuse of the mechanism. Without identification, individuals or organisations can pursue malevolent agendas without being held accountable. The same applies in terms of contesting the removal of content. Transparency of the process is vital; and the ability to identify both parties is essential to a viable appeal process. Nonetheless, as identified by the Information Commissioner's Office, "it is important that you only request information that is necessary to confirm who they are". This ensures that any request for information is proportionate.

Yoti would be able to facilitate such identification. Using Yoti, an internet service provider would be able to request a proportionate amount of information permitting it to ascertain the identity of an individual. Both the user and the individual would receive an irrevocable receipt of the transfer of information, thus disincentivizing the abuse of the content removal mechanism.

- Pseudonymisation

A number of people choose to express themselves using a pseudonym or anonymously. This is often the case on social media platforms such as Twitter, Facebook. On some occasions users abuse this and use their veil of anonymity to spread illegal content, commit crimes of racial abuse or hatred.

A way to reduce the latter and nudge appropriate behaviours would be to require identification when people create an account. A person could still act online with a given name and interact under this name. However, the service provider could have the ability to identify the real name of the person, in instance of unlawful behaviour.

Summary & Recommendations

In summary, it is clear that age and identity verification can contribute to online safety. Current knowledge based self assertion of personal details, entered into web registration forms, is a deeply flawed approach. It is easy for bad actors to create fake accounts and commit fraud and online crimes.

The updated age verification approaches enables the safeguarding of young people and age appropriate access content that is for under 13, under 18 or over 18.

We applaud organisations, like the NSPCC and IWF, for working towards safeguarding vulnerable individual on the internet. We are proud to enable young people to flag and anonymously request indecent images to be removed.

We support the effort of the Government to develop a safer digital environment for all the population and we believe that, just as they mention in the Internet Safety Strategy - Green paper, *all users should be empowered to manage online risks and stay safe.*[1254] Likewise, we believe that digital identity should be accessible for all, hence our digital identity app is free for all users.

By verifying users' identities Yoti can make online dating and classified sites safer and enable polls to ensure there is one person one vote. Having a verified name of users linked to their biometrics and Government issued identity documents is a strong deterrent to fraud and crime.

Digital identity will help to make Britain's digital economy a safer place. Once consumer set their identity they will be able to interact and use it for many purposes, including age verification, proving they are genuine user to vote anonymously and be able to prove who they are online.

May 2018

[1254] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf

YoungMinds and The Children’s Society – written evidence (IRN0025)

Written evidence to be found under The Children’s Society

Dr Nicolo Zingales, Professor Pinar Akman and Dr Orla Lynskey – oral evidence (QQ 83-92)

Transcript to be found under Professor Pinar Akman