DATA PROTECTION - ONLINE DISCUSSION

POST E-1
E-Report *December 1998*

In July 1998, the Parliamentary Office of Science and Technology (POST) initiated its first ever parliamentary online conference. This was designed to solicit the views of relevant stakeholders regarding the issues surrounding the Data Protection Bill currently before the UK Parliament. The object of the exercise was not to influence the content of the Bill but rather to provide direction during its subsequent implementation after enactment. A secondary, though separate, function of the exercise was to contribute experimentally to ongoing developments concerning 'electronic government', as discussed in the 1998 POST report[1].

INTRODUCTION

Fifteen participants, excluding a discussion facilitator and a technical housekeeper, contributed via e-mail to the discussion over a five-week period from 1 July to 7 August 1998. The exercise was hosted on the web site of UK Citizens' Online Democracy (UKCOD), an independent, non-partisan public online forum set up in 1995 as a public space for political discussion linking citizens with one another and with their representatives (http://www.democracy.org.uk). The discussion was facilitated by the Director of Studies of The Hansard Society for Parliamentary Government, an independent, non-partisan educational charity, whose President is the Speaker of the House of Commons (http://www.hansard-society.org.uk). The online context allowed all participants to express their opinions on subjects proposed by the facilitator and to introduce new topics themselves. In all there were 12 separate topics discussed through 33 distinct contributions from participants.

The first section of this report summarises the discussion, draws out recurrent themes and determines whether a consensus was reached on any of the issues surrounding the new legislation. The second section examines the strengths and weaknesses of running such a virtual conference and offers some preliminary proposals for approaching future parliamentary online conferences.

THEMATIC CONTENT OF THE DISCUSSION

The initial conference agenda invited participants to discuss the principles of the Data Protection Bill and to identify potential obstacles to its implementation. After this, new topics were introduced and responses considered and returned with comments that often pushed the consultation in a new direction. There follows an outline of agenda topics and an indication of how the discussion evolved.

Is there a conflict between the principle of individual privacy and that of efficient government, including detection and prevention of fraud? (5 submissions)

The discussion began with the acknowledgement that the issue of data protection is concerned with threats to human rights that may arise from electronic processing and dissemination of data. Accordingly, the first data protection principle states that all information contained in personal data should be 'fairly and lawfully' obtained and processed.

Many of the topics discussed below follow on from this principle. In terms of the potential conflict between the principle of privacy and the need for efficient government, most of the five respondents to this topic agreed with Francis Aldhouse, Deputy Data Protection Registrar (UK), that the protection of privacy is an objective of democratic government whereas efficiency is a measure of how well government fulfils its objectives. Privacy rights may conflict with anti-fraud measures but the latter are instruments of government and not an end value. Ann Cavoukian, Information and Privacy Commissioner for the Province of Ontario, Canada, concurred with this view, stating that it informed the approach to identifying welfare recipients in Toronto. The city introduced encrypted rather than full image biometrics to detect fraud without sacrificing privacy.

Despite this positive example, Sarah Tanburn, Director of Strategy and Information at Hertfordshire County Council, was concerned that the current law should not be designed to comfort the criminal at the expense of others. She asserted that in areas such as health and crime, where multiple agencies are involved, it is essential that they share information to be effective. Although Clare Wardle, Head of Intellectual Property at Post Office Legal Services, agreed, she also pointed out that the law should restrict agencies using/sharing information that is not essential to the task at hand.

The discussion appeared to indicate that individual

[1] ***Electronic Government - IT and the Citizen*, Parliamentary Office of Science and Technology, February 1998**

privacy and government efficiency are not necessarily incompatible. However, in the implementation of the Act, the rights of the data subject must constantly be weighed against any perceived advantages of efficiency. To this end Ron McQuaker, Director of Exxel Consultants Ltd, suggested the need to determine at the outset the data required for efficient government. What should be included should be determined by the purpose for which the data are intended. This purpose must always be legitimate and lawful as determined by social and political judgement.

With regards to the general principles of data protection, Michael Spencer, a consultant on data protection and civil liberties, noted that the time to discuss these had been before the Bill had been drafted. As this stage had passed and the Bill as it stood was hugely disappointing (due to the widespread exemptions and lack of statutory privacy) the discussion should focus instead on how defects can be remedied through secondary legislation. Wardle addressed this comment and suggested that, in particular, s.67 contains provision for a huge amount of secondary legislation to conform to the EU directive.

To what extent should the Data Protection Registrar (DPR) implement codes of information ethics? (6 submissions)

Many of the submissions on this indicated that contributors wanted to reformulate the original agenda question so that they could discuss more generally the role of the DPR and not just ethics codes. Most of the six submissions on this topic advocated a proactive role for the Registrar in devising, implementing and enforcing codes. However, the UK Government has refused to give the Registrar the independent power of audit or site inspection that exists in many other countries. Every other country in the EU has interpreted this power as necessary for compliance with the EU Directive on Data Protection, pointed out David Wyatt, a Data Protection Manager with the Norwich Union Insurance Group.

Several other concerns were raised. First, it would be extremely difficult for the DPR or the statutory sector alone to implement standardised codes of information ethics, because massive amounts of private information are held elsewhere, particularly in the financial sector, as Tanburn noted. The solution proposed by Sarah Stockman, a Consultant and Data Protection Manager for Woolwich plc, was that in sectors where the Registrar has no expertise and little resources for enforcement, it would make sense to collaborate with the industry to devise a set of codes and then to encourage the industry to self regulate. Arguably this is already in operation in some private sectors. Cavoukian pointed out that sector-specific codes are in effect for the banking and credit reporting sectors in Canada and that the Canadian Standards Association has developed a model privacy code that can be adopted by the private sector.

How far can privacy enhancing technologies (PETs), such as encryption, meet the aims of data protection? (10 submissions)

This question elicited the highest number of initial responses and subsequent interchanges from contributors, perhaps because, as Cavoukian noted, the degree of control that a data subject exerts over his/her information is at the heart of the issue of data protection, and PETs enhance control as they allow for the separation of 'true' identity from online identity. Several recurrent themes emerged throughout this discussion. First, although PETs can help to protect electronically stored data they should not be regarded as sufficient. Indeed, six contributors asserted that they should be viewed as supplements, albeit important ones, to a regulatory framework. In addition to policy and PETs, two respondents agreed with Aldhouse that the culture of an organisation/sector should foster an awareness of data protection issues and propound the view that data protection is good business practice and not an expensive nuisance. Unfortunately, it appears that many businesses fail to adopt this stance as concern with costs colours their perspective.

Industry/sector emphasis on the expense of PETs was another theme in the exchanges. Not only is there the cost of installing PETs but, for example, in the marketing industry, fear of income lost through the less personalised campaigns necessitated by data restricted by PETs. Wyatt asserted that the benefits of PETs (privacy protection could be sold as providing a positive commercial advantage) should be promoted, perhaps via the Commissioner's TV campaigns to the public and within periodicals read by computing specialists.

The industry image of PETs must be transformed from one of incredibly expensive technologies to just one element in the repertoire of good business practices necessary to treat citizens/consumers fairly. Several felt that the government has done nothing to promote this positive view and, in the opinion of several contributors, has actually contrived to make the issue of data protection as boring and burdensome as possible. Finally, it was acknowledged that real cost of PETs could be significantly reduced if installed at the outset of a project. As the Director of Policy and Research at DEMOS, Perri 6, noted 'the costly bit is PETing an existing privacy-disrespecting system.' This point reinforced the need to change the perception of these

technologies and thus obviate the updating of systems in the future.

What is the public's perception of the issue of data protection? (3 submissions)

This topic was introduced by Tanburn who wondered if anyone knew of any research on how the public views the issue and whether any myths had taken root. Perri 6 responded that he had just produced such research in a Demos study entitled The Future of Privacy based on a representative sample of UK adults. Among his findings was that the existence of the current Data Protection legislation is still the main reason[2] for the public's trust in the handling and use of personal information by organisations. In addition, the results indicate that the public is more concerned about the sharing of data within the public sector than about within strategic alliances across the retail sector in 'loyalty' card schemes.

Specific myths that the public appears to hold include the belief that GP surgeries and the NHS are the institutions most likely to respect confidentiality. In fact, GP surgeries are very 'leaky', while many criticise the quality of security provision in NHS experiments in ICTs. Another prevailing myth is that information, such as the type of newspaper that one reads, is not very personal and therefore trivial. In reality, direct marketers can infer quite a lot about an individual's wealth, aspirations and socio-economic class from this one piece of information. This could have disastrous consequences if shared with, for example, credit rating agencies.

Richard Kingham, Managing Partner of the London office of Covington & Burling, also contributed to the discussion of Tanburn's topic and added his perception that consumers appear to be increasingly concerned about the issue of data privacy. He asserted, however, that this awareness might be less developed in the UK and the USA than in continental European countries. Perri 6 responded that, although his survey did not directly address this assertion, he was inclined to disagree as the respondents were surprisingly discriminating between organisations, reasons for their trust and what they trust organisations not to do with personal information. Indeed, the sample evinced strong latent concern, with the gradient of risk perception positively correlated with age and education.

[2] cited by three quarters of the sample

How does the Bill deal with the issue of data matching? (2 submissions)

Perri 6 stated that it is not the quantity of information held on a data subject but the fear of unjust inferences from this information, known as data matching, that provoked the strongest concern among the respondents of his survey. It appears that the current Bill will do nothing to alleviate these fears because, as Spencer noted, the provisions included to control data matching between government agencies are far behind those in comparably advanced democracies such as Germany or Australia. The Bill offers only two options with regards the dangers inherent in data matching. The first is for the Secretary of State to formulate an order requiring the Commissioner to consider whether it is likely 'significantly to prejudice the rights and freedoms of the data subject.' The second is for the Commissioner to draft a code of practice with which public officials should comply even though it does not carry statutory authority.

What are the implications of the Bill for the international exchange of data? (7 submissions)

This subject stimulated the lengthiest responses from contributors, including one from an expert who joined the discussion solely to contribute to this topic. Several related issues became apparent during the exchanges. Perhaps the most contentious issue concerned Principle Eight of Schedule I of the Bill which forbids the transfer of personal data to any country outside the EEA that does not provide an 'adequate level of protection' as defined in general terms by Part II of the Schedule. This issue was first raised by Spencer. The facilitator attempted to focus the ensuing discussion by asking if anyone could offer a working definition of 'adequate level of protection' or identify possible problems that it could cause for the global flow of information.

Spencer noted that deciding initially what is adequate would be the responsibility of the data controller. This will, however, always be subject to review by the European Commission which could decide that a given country does not offer adequate protection. Kingham posited a more instrumental view and asserted that there are two components to determining the adequacy of data privacy protection in a non-EEA country to which data are transferred. First, the substantive rules applicable to the transferee should be essentially the same as those that apply under the EU Directive. This can be accomplished by any, or a combination, of three methods: national statutes or regulations in the non-EEA country, industry or sectoral codes of conduct, or

provisions of contracts between the EU based transferor and the transferee.

The second adequacy component concerns rule enforcement mechanisms. This is more controversial as problems may arise if the authorities insist that these mechanisms mirror those in the EU. Wyatt argued that the Bill is flawed, as it appears that conditions in Schedule IV of the draft nullify a need for compliance with the adequacy conditions of the Eighth Principle. He identified two parts of the Bill where this is the case. First, if the processing operation is claimed to be necessary for the performance of the contract then there is no restriction on the data transfer. The controller simply has to ensure that a contract exists. Second, if the data subject has given, or implied, consent to the transfer, then no restrictions apply. However, often the subject cannot know if the data controller bases its operations in a non-EEA territory. This could cause problems. For example, would a Mr Rushdie be concerned about providing his name and address to a call centre operating in Iran?

These clauses appear to have been included to minimise the cost of activities required to be in compliance with Principle Eight and, as a result, the principle provides protection only at certain times. In addition, pursuing redress of any infractions of the regulations in court would most likely require a data subject with 'deep pockets and a strong will.'

Concerning the topic of potential problems arising from Principle Eight, Scott Blackmer, a US-based lawyer who specialises in international technology practice, drew attention to the scope of the problem involved in the development of accepted practices regarding international data flows. Several factors conspire to thwart protection, including the incredibly dynamic evolution of computer and communications technology. He noted that current laws tend to focus on the old 'mainframe' model in which a data controller in Europe sends data to a mainframe processing centre outside the EU. In this conception there is a clear chain of decision making, routine practices and local establishment and accountability. This model still applies to many data processing transactions (credit cards, electronic funds transfers, travel reservations, etc) and for these types of exchanges it should be relatively easy to establish practices that ensure adequate protection. He contrasted this with the emerging information technology model of decentralised computing in a global group, using common software platforms, linked by private lines, the Internet, intranets and extranets. Alongside these were increasingly sophisticated techniques of data warehousing and data mining and the hundreds or thousands of employees who have access to this data.

Security controls do exist in these multinationals as managers train and monitor employee transactions, albeit mainly to avoid the disclosure of commercially sensitive information, and have recently begun to include personal privacy restrictions. However, in this scenario it will obviously be more difficult to develop practices to ensure adequate protection. Blackmer's recommendation was, therefore, for the EU to proceed pragmatically and incrementally to ensure credibility and to focus on where the greatest risks to privacy actually arise. It should be remembered that, as there is currently no standard definition of 'adequacy' in the various derogations in the Bill, multinationals are left to make their own determinations.

To this end, there are several associations (e.g., the CBI and the International Chamber of Commerce) that are preparing model contracts for transborder data protection. These are valuable in that those that are engaged in the transactions must be heard to ensure practicable solutions. Blackmer hoped for an informed debate on the issue and expressed optimism that solutions could be found. Stockman was also concerned about the issue of model contract clauses and their ability to meet the adequacy requirements of Principle Eight.

A related theme arising from the subject of Principle Eight concerned the data transactions occurring specifically in North America, especially the US. Four people offered detailed comments on this issue. Spencer said that it was this aspect of the Directive that has provoked 'panic and outrage' in the USA, with Congressional complaints about the EU assuming extra-territorial jurisdiction. The issue is being taken very seriously in the USA, mainly because of the potential for trade lost due to privacy restrictions. Thus, three of the contributions pointed to the laws (or lack thereof) already in place in the USA and offered suggestions on how it could expand these to ensure compliance. It was noted that, at present, there is no omnibus Privacy Act, (nor is one likely in the future), and that there are many gaps in the patchwork of federal and state laws. Kingham further listed some government enforcement mechanisms currently under consideration, such as a federal law on confidentiality of medical records. However, he was most optimistic about initiatives by the Federal Trade Commission (FTC): a quango charged with the enforcement of the broad consumer protection law that prohibits 'unfair' or 'deceptive' practices. Recently the FTC has launched enquiries into the protection of data privacy in electronic commerce and thus may become the guarantor of data privacy, at least

in some sectors.

Aldhouse approached the issue from a different angle. He first asserted that European law sees data protection as a development of the right to private life guaranteed by Article Eight of the European Convention on Human Rights (as well as other documents). In this context, it is proper that the EU ensures that the rights of individuals are not circumvented by the exportation of data for processing elsewhere. To this end legal duties can be imposed on those who export to countries that do not ensure adequate protection. Loss of trading activity due to data flow restrictions has been recognised as legitimate by Article 14 of GATT and it is this consequence that is the principle US concern.

Aldhouse pointed out that all developed western states recognise the need for rules on the processing of personal data as follows from the general acceptance of the 1980 OECD Privacy Guidelines. The real issue is how these are to be satisfied within the different legal and political cultures of member states. He suggested that if all the member states approached the issue by first requiring each other's compliance with the guidelines, then there might be less difference between Europe and North America than some would insist upon. Cavoukian (from a Canadian perspective) appeared to concur and also noted the gaps in legislation within the federal system of Canada. However, the government there is committed to introducing more comprehensive legislation by the year 2000. This will most likely be based on the Canadian Standards Association Model Privacy Code that incorporates the fair information practices of the OECD. The comments recorded in the seven total exchanges concerning the international transfer of data showed that the contributors found this topic the most intractable and confusing of all the issues surrounding data protection.

How do the exemptions for law enforcement agencies under the DPA 1998 affect individuals' right to respect for privacy? (2 submissions)

This topic was introduced by Noorlander, a member of the independent human rights organisation, JUSTICE, which is about to publish a report on proactive policing methods. Part of this deals with the gathering and processing of criminal intelligence data, so he was interested to hear what the other members of the conference thought about the widespread police exemptions included in the DPA. Proactive methods or 'intelligence-led policing' involve the police gathering information on suspected criminals, to catch them in the act rather than to investigate offences after they have been committed. As a policing method, this appears to be effective but also raises serious human rights issues.

Criminal intelligence is of variable reliability and the category of people on which it can be held is broad. Thus, an effective legislative framework is needed to protect individual privacy. Although the police must comply with data protection principles, they are exempted from three key provisions of the law whenever their application would harm their activities. The first principle of 'fair and lawful processing' need not apply in some instances, nor the 'subject access' or 'non disclosure' principles. It is difficult to assess the impact of such exemptions because of the absence of public information and the general secrecy surrounding this area of police practice. Noorlander said that JUSTICE felt that a comprehensive inquiry is needed into the holding and processing of criminal intelligence information by law enforcement agencies, to determine the optimal balance between policing needs and the interests of the individual. Stockman also wished to voice her concerns over the extent to which law enforcement and other regulatory agencies use their powers. In her experience, the police, Department of Social Security, Child Support Agency, etc. often contact financial institutions for information regarding their customers. In many circumstances these people are not involved in criminal activities but are innocent bystanders.

Here, the need to minimise fraud conflicts with the responsibility of confidentiality to customers. Most large organisations have a well-developed policy to filter such requests but sometimes, personal data is transferred. In considering the case of Elizabeth France, who was trying to open some of the files held by MI5/6, one contributor concluded that blanket exemptions may not always be in the best interests of the individual and that tighter controls are required.

What are the ethics surrounding the issue of the disclosure of personal information? (2 submissions)

Joanna Tallantire, Home Affairs Officer from The National Federation of Women's Institutes, had learned from the Home Office that the Driver and Vehicle Licensing Agency (DVLA) discloses relevant information regarding the owner of a vehicle if there is reasonable cause. This is sanctioned by Regulation 15 of the Road Vehicles Regulations 1971 and raises the ethical concern that the Home Office has devolved responsibility for compliance with the Data Protection Act 1984 guidelines. Simon Chalton, a solicitor and

consultant to Bird & Bird, responded by stating that the ethics involved in DVLA disclosures can be measured against the first principle of data protection. This requires personal information be obtained and processed fairly and lawfully. Thus, it is fair to disclose information if the disclosee has a legitimate interest in requesting it, for example to pursue a legal claim, and it is lawful if the disclosure respects civil, criminal or statutory obligations.

What are the implications of the DPA 1998 for personnel records especially exemption of confidential references? (4 submissions)

This encompasses several related topics and there was a clear chain of responses from contributors indicating how the issue evolved. Chalton took up the clause dealing with personnel records relating to the definition of manual files and relevant filing systems and exemptions. One current interpretation of the definition of a 'relevant filing system' excludes files on a data subject which contain unstructured material. Chalton (and others) asserted that this definition seems unsustainable and unfair as the unstructured material may be in the form of letters, reports etc. that may contain sensitive data, clearly relating to the individual in question. Indeed, the interpretation is an invitation to create 'black' unstructured files, containing unfair or inaccurate material, and then claiming they are exempt. Wyatt agreed that the data protection regime appears to favour the data controller over the data subject. Subjects are often not in a position to identify whether the controller has provided all the information to which they are entitled. Additionally, from a commercial perspective, the main concern in planning for the legislative changes will be to minimise costs. Accordingly, debate has centred on whether existing manual files are bound by the Act as due diligence would then be required to ensure compliance, with major cost impacts. The Data Protection Registrar has stated that such an exercise will not be necessary - files should be screened as used. This leaves the question as to whether the legislative drafting will permit this without challenge. Thus, the former interpretation, exempting manual files, must be considered in this context. If the definition is proven "*unsustainable and unfai*"' it may force a due diligence regime on organisations. This would be difficult to police in light of the Commissioner's current powers, or lack thereof.

Anthony Bourne, a lawyer working for ICI, replied to the contributions of both Wyatt and Chalton. He asserted that accepting the case for subject access to information processed automatically and arguing that a sensible manager might willingly give access to paper files, is a long way from agreeing that the traditional right to hold information in written form must henceforth always be balanced by a corresponding duty to allow subjects to inspect it. Similarly, with regards confidential references, it may be right to encourage referees to be more open with those about whom they write but to make this compulsory risks the opposite effect - it may mean that the 'true' facts are exchanged orally rather than in written form. Finally, Wyatt responded to Bourne's contribution regarding his previous commentary on confidential references. There is agreement that references should be factual and accurate. Ensuring the discovery of the content of such references is one means to ensure this. However, the exemption within the new DPA makes discovery of error more difficult for an individual. Thus, although confidentiality is preserved, the Act will favour the organisation at the expense of the individual.

What is the definition of a 'nominated representative' as used in the Bill? (2 submissions)

Addressing the fine detail of the Bill, Stockman asked for information concerning fellow contributors' interpretations of the definition of a 'nominated representative' as used in Schedule 1, Part II, 2 (3). She had spoken with an authority involved in data protection who seemed to think that every third party directly involved in the provision or processing of personal data would need to be specifically named. Bourne replied that this must have been a misunderstanding. The 'nominated representative' is referenced in the s5(2) requirement that a data controller established neither in the UK nor in any other EEA State 'must nominate for the purposes of this Act a representative established in the United Kingdom.' The identification of any third party will rarely take place and is necessary only when it is deemed relevant to guarantee fair processing. The test to apply is whether, in the specific circumstances, knowing the identity of a third party processor would be regarded by data subjects as a relevant factor in deciding whether they regarded the process as 'fair.'

What is the relationship between data protection and freedom of information? (1 submission)

This subject was introduced by the facilitator. Aldhouse alone addressed it. He acknowledged the relationship between the proposed freedom of information legislation and that on data protection. The Human Rights Bill currently before Parliament will provide the context to assess when one principle conflicts with the

other. However, the development of information policy in general would be best served by the enactment of Freedom of Information legislation, as the best way to deal with the potential conflict is through a statutory framework. He stated that the Registrar also subscribes to this opinion and believes that an effective working relationship could and should be developed between the two Commissioners.

How will the data protection legislation affect investigative journalism? (1 submission)

The final topic proposed by the facilitator brought the discussion around full circle as it was concerned with the first principle of data protection - with which the consultation began. Chalton pointed out that the first principle, which requires all personal data to be obtained and processed 'fairly and lawfully', may be diluted or made undiscoverable or unenforceable by the proposed exceptions. By way of example, he pointed to the reduction in the rights of data subjects *vis a vis* investigative journalism which will occur through the substitution of the 1984 Act by the new Bill.

THE VALUE OF THE ONLINE DISCUSSION

The value of new information and communication technologies (ICTs) to the democratic process has been asserted but less frequently tested. POST, in its report on *Electronic Government*, suggested that use of ICTs could help to build closer links between citizens and their representatives[3]. The Dutch Ministry of the Interior's excellent guide to the use of the Internet in interactive policy-making[4] provides several practical recommendations, based on Dutch experience, for the organisation of online public consultations.

Some online discussions are directly open to the public; others involve only invited experts. With yet others, there is an implied or explicit commitment by the authority sponsoring the exercise to feed the public's views into the policy-making process. Open public discussions can be generated by citizens (such as those which take place on the Open Forum of the UK Citizens Online Democracy site: a virtual Speakers' Corner) or by representatives, such as the Downing Street web site. This has invited the public to enter into dialogue on topical questions of the day, such as the discussion on relations with China, in which the UK and French Prime Ministers and the German Chancellor exchanged views with members of the public. The value of such all-inclusive and open-ended online deliberations has yet to be fully researched, and questions need to be asked about how they are produced and structured, the extent to which members of the public have real access to them and participants' perception of their value. The safest observation to be made at this point is that without ICTs there would probably be fewer fora for public discussion.

Online public consultations are different from public discussions in that the former appear to be connected with the policy-making process. For example, in January 1997, the London Borough of Brent, via the UKCOD web site, consulted its citizens on the proposed level of the following year's local council tax. It was made clear that the votes cast by participants were advisory rather than being in any sense binding, but the council entered the consultation on the basis that citizens, provided with online information resources, were likely to come to a wiser public judgement than if they were not so consulted. In 1997/8 the UK Cabinet Office placed its *Right To Know* White Paper on UKCOD's *Have Your Say* web site (www.foi.democracy.org.uk), inviting members of the public for the first time to participate in online pre-legislative scrutiny. The extent to which either of these experiments in online consultation contributed meaningfully to the democratic process is a subject for research. Preliminary examination of the latter exercise suggests that significantly more individual citizens participated in the consultation about this White Paper than is usually the case. This may well point only to the success of the exercise as an online *discussion*, permitting a broader range of views to be aired, than as an online *consultation*, in which comments made may be expected to have any impact upon subsequent policy.

The best examples of online public consultations are from the Netherlands where a strong tradition of civic consultation preceded the use of ICTs. The 1996 'Besliswijzer' consultation on land use in North Brabant province is a particularly well-researched experiment in public consultation, comparable with the Data Protection discussion which is the focus of this report, in that its participants were invited. (Jankowski *et al*, 1997) A comparable UK exercise in online deliberation, carried out as a discussion rather than a consultation, was the Scarman Trust/UKCOD online debate on European Monetary Union (UKCOD, 1996) Both of the above-mentioned online discussions can be regarded as precedents to the Data Protection online conference; the strengths and weaknesses of the discussion reported here can be measured in relation to these earlier experiments.

[3] **see footnote 1**
[4] ***Electronic Civic Consultation*** **(The Hague, 1998)**

Important as the differences are between various types of online discussion/consultations, a much greater contrast is that between virtual conferences and face-to-face meetings. Leeuwis has suggested eight ways in which electronic forms of debate have potential advantages over conventional forms. These include the possibility of including a larger number and types of participants, taking part on a more equal basis; more time for discussion to take place, for arguments to be stated fully and for the agenda to be broadened; the greater availability of information for participants to consider; and more opportunities for those outside the decision-making elite to participate (1998). These advantages, and methods of realising their potential, need to be assessed empirically. In the case of the Data Protection online conference, the relevant contrast is with a hypothetical meeting hosted by parliamentary officials or by an MP, perhaps on behalf of a pressure group, within a parliamentary setting. Such meetings tend to be limited to a select group of invitees. Few of these will have an opportunity to contribute at length, to influence the agenda or to have access during the meeting to all of the information sources to which they might want to refer. These disadvantages of a one or half-day face-to-face meeting might be outweighed by other advantages of physical presence, such as the ability to form a judgement about the credibility of a point of view by meeting a person advocating it; the social opportunity before, during and after the meeting to exchange informal comments with participants and perhaps to generate networks that will serve a greater subsequent use than the meeting itself; a sense of being physically close to decision-makers, rather than being virtually connected to them, but possibly ignored.

These benefits and disadvantages need to be researched within the specific context of Parliament-based discussions, from the both perspective of participants' subjective perceptions (social psychology) and criteria of effective political influence. Future research will be carried out within the next year to examine both participants' perceptions and the political value of face-to-face and online meetings. Although, as will be shown below, the level of feedback from the online Data Protection conference was too small to allow conclusions, it is interesting that, when asked whether they had attended meetings or conferences on Data Protection, all of the respondents stated that they had. When they were then asked whether they found participation in an online conference more or less convenient, half of the respondents said they found it more while the other half found it less convenient.

Servers and software to host the discussion were provided by UKCOD. The server was a Sun Solaris box, running the Apache web server, majordomo mailing list server and Omniformum software which provides a common interface between e-mail and web for the purpose of discussion and message archiving. Each participant was subscribed automatically to the mailing list upon receipt of his or her agreement to take part. Subscription to the list was passport-protected. The overwhelming majority of contributions to the discussion came via e-mail, although the facility to post via the web was available. Submissions were automatically archived on the web site, but were accessible only on production of a user name and password. A number of web pages were provided offering background information on the subject of the discussion. The main technical problem encountered resulted from e-mails being bounced back from participants due to configuration problems with the mail servers at their end; all participants on the parliament.uk domain experienced initial difficulties because configuration problems prevented them from receiving e-mails. A considerable amount of time had to be spent in the opening stage of the discussion correcting wrongly set-up configurations for individual participants.

94 invitations were issued to participate in this online conference. 42 people responded positively, although with 4 of them, e-mail could not be delivered to the address they gave, so they were unable to participate in the discussion. This left 38 participants: 40% of those invited. One might have expected specialists in Data Protection to be significantly more electronically connected and interested in electronic discussion than experts in most policy areas. Nonetheless, 4 of those originally agreeing to participate could not be reached by e-mail, while one major national body, concerned on a daily basis with the international flow of data, declined to participate on the grounds that it did 'not have ready access to external e-mail and the Web.' In general, however, the participants' level of technical experience was significantly higher than the wider population's. According to the registration questionnaires filled in by all participants, 95% had over 6 months experience of using e-mail; 71% had participated in previous online discussions/conferences, (with 41% having done so often); and 41% were subscribers to at least one other e-mail discussion list.

The level of participation (defining this as registration for the online discussion, not necessarily as active contribution during the discussion) was satisfactory, given that the invitees were all busy specialists. Compared with the Scarman Trust/UKCOD EMU debate, in which 166 invitations were issued to specialists, leading to 45 registrations (27%), the take-up

rate was high. Against the North Brabant land-use online consultation, for which invitations were issued to 100 members of the public, of whom 87 (87%) registered, the participation level was, however, low. This can probably be explained by the specific local interest in the case of North Brabant land use (in the case of the Data Protection Bill participants could pass only retrospective comment on the policy and were confined to discussing its implications) and also by the fact that members of the public might have more time to participate in electronic discussions than senior specialists.

15 (39.5%) of the registered participants contributed to the online discussion; 23 (60.5%) did not. There was a higher percentage of contributions from participants in the EMU debate (47%), although nearly half of these came from the highly proactive moderator who was concerned to keep the discussion flowing. In the Data Protection conference the moderator's contributions were far fewer – while neither the moderator's contributions, nor those from POST and UKCOD counted as 'participation'. In the North Brabant consultation, 45 (52%) of the 87 participants contributed, although over half of all of the 298 contributions were made by just 8 contributors. In the case of the Data Protection discussion, those who did contribute tended to do so between one and four times. There was therefore an even spread of contributions, with 33 distinct submissions coming from 15 contributors, with 7 making multiple contributions. (A sixteenth contributed only to explain that she did not have time to contribute to the discussion; this has not been included in the statistical analysis.)

Why did most participants not contribute to the discussion? Unfortunately, there is no feedback information on this, but three speculations are offered for consideration. Firstly, the online conference took place during July and early August - some registered participants who might have contributed may well have been away from their offices and/or computers. Secondly, it is usually the case in formal discussions, whether offline conferences/seminars or online, that most of those attending prefer to listen and gather information rather than play an active role as a speaker or contributor. In many discussions there are people who are good listeners and who prefer to accumulate than contribute information. It is often the case in face-to-face meetings that those in attendance say that they would have raised a point or question but it was raised by somebody else. In physical meetings, especially parliamentary-based ones, much of the time is often taken up by an address or lecture by a single politician or specialist panel; in online discussions there is more egalitarian access to the discussion forum, but still some participants probably feel more comfortable as observers rather than active participants. Thirdly, it may be that some participants were not clear about the point of the online conference. Were they addressing each other or seeking to influence Parliamentarians? What was the point of discussing a piece of legislation after Parliament had decided upon it? Why should experts with an interest in a specific aspect of Data Protection bother to contribute to discussion about aspects or general principles which seemed to be of little relevance to them? The motivation to enter into discussion about public policy will rarely be an interest in the abstract benefit of deliberation; perhaps participants were unclear about quite how contributing would serve their interests.

A more optimistic re-framing of the previous question might be, "Why did so many of the registered participants take time to contribute and how did they see the benefit of taking part?" Unfortunately, the feedback questionnaires, which should have been sent to all participants soon after the conclusion of the conference, were not sent for several weeks and only 4 completed questionnaires were returned. From these, the main benefit of the conference appeared to be its open agenda, but, perhaps contradictorily, all 4 respondents agreed that the conference lacked focus and also that there was insufficient interaction between contributors.

The latter point may possibly have been helped by more proactive moderation, with the moderator taking a much more energetic role in urging participants to take up points made by one another - particularly when there appeared to be disagreements. The view of the present writer (both as moderator and reporter) is that, whereas proactive moderation is useful in a public online discussion or one concerned mainly with political opinions, the technical nature of the Data Protection discussion limited the likelihood of the kind of combative interactions often associated with vigorous debate.

There was a close compatibility between the subjects discussed ('discussion threads' in the jargon of e-discussion) and the subjects that participants suggested in their registration questionnaires for inclusion in the conference agenda. The length and flexibility of an online conference diminishes the significance of a highly-structured agenda. At the beginning of each week, the moderator proposed themes for discussion, but participants were free to raise their own new themes or return to earlier ones. Some contributors made single submissions that covered subjects from several threads. This could be confusing and unhelpful to a focused

discussion. In face-to-face meetings, there are often similar contributions, particularly when contributors know that time is limited and they might have only one opportunity to speak. Consequently, they will sometimes try to address aspects of the agenda that have passed or are yet to be reached. The subjects proposed by the moderator were selected on the basis of their prominence in the registration questionnaires. Both PETs and the international flow of data were two of the most frequently raised subjects in the registration questionnaires. These also attracted the most contributions to the online discussion.

LESSONS FOR FUTURE ONLINE DISCUSSIONS

1. The timing of this discussion in relation to the legislation in question was not ideal. Participants in discussions about parliamentary affairs, whether concerned with legislation or broader policy deliberation, are likely to feel that what they are doing is more meaningful if their comments might influence Parliamentarians. This is not to propose a form of direct democracy whereby elected representatives cede power to, or share power with, unelected groups of online deliberators. A function of good online discussions in a parliamentary context should be to provide a forum for extensive deliberation involving those with special knowledge, and to make available the record of such deliberation (both in full and in a summary report) to Parliamentarians who are concerned with the making and scrutiny of impending legislation or policy consideration under discussion. For example, in the case of Data Protection legislation, the benefit to MPs of having access to the record of this online conference would be to assist them in their understanding of relevant questions and to expose them to problems identified by experts.

2. A similar use of an online conference might be linking it to a Select Committee enquiry, examining a particular aspect of policy. Contributions to the online discussion would not constitute official evidence to the committee, but it is quite possible that committee members could benefit in their knowledge of issues by having access to online deliberation. At the same time, participants in the online discussion would have a greater sense of not being too late to have any influence upon the deliberations of Parliamentarians.

3. A strength of this discussion was its impartiality. That is not to say that participants had no strong views about Data Protection policy, but, quite clearly, they were not selected because they had one view rather than another. Recognition of such impartiality requires full confidence in the body organising and monitoring the discussion. Although such non-partisan neutrality is fundamentally necessary, future discussions need not consequently be bland or lacking in controversy. Indeed, a possible weakness of the Data Protection discussion was the technical nature of much of it and the sense that nothing said would be likely to have an influence in the real world of politics. Future online discussions should not avoid potentially controversial areas of policy - particularly ones about which expert opinion is strongly divided. (Examples could be genetic engineering, European monetary union, welfare reform or environmental policies.)

4. The experts selected for the Data Protection discussion were all high-level practitioners with a degree of peer knowledge and respect. The high quality of the discussion content certainly reflected this. Future online discussions might include more people on the front-line of policy delivery, as well as those on the receiving end of legislation or policy. For example, an online discussion about *in vitro* fertilisation policy could involve nurses, patients and non-specialist GPs, as well as specialist consultants, scientists and experts in medical ethics. Similarly, it would be sensible, in any future online discussion on citizenship education, to invite school students, community workers and school teachers, as well as the more obvious policy-makers.

5. Participants in the Data Protection discussion were invited to take part under the aegis of Chatham House Rules[5][6] In the event, no part of the discussion displayed a confidential nature and there is no evidence that there would have been fewer contributions had the discussion been on the record. (In the event, participants agreed that the summary report could attribute points made to named contributors.) Future online discussions should be conducted on the basis of a general principle of attribution (although the discussions should still remain closed to invited participants.) Only when discussion subjects are manifestly sensitive, and freer

[5] **These are named after Chatham House, the location of the Royal Institute of International Affairs, which drew them up to govern the conditions under which comments made by participants at its meetings might be reported. Basically, the rules permit quoting of comments provided that this does not directly or indirectly identify the individual who made them.**

discussion might be served best by the protection of confidentiality, should Chatham House Rules be used in future.

6. Longer-term consideration could be given to open discussions, in which any member of the public can submit views and add information - as happened with the Cabinet Office-supported Have Your Say consultation on the Freedom of Information White Paper. Members of the public might even be invited to propose the actual subjects for online discussion.

7. The length of the Data Protection conference (five weeks) allowed the discussion to take off and cover most of the subjects of major interest to participants. From the limited feedback by participants, all agreed that its length was 'about right', although at the end of the conference several participants expressed an interest in continuing the discussion on an informal list. This is welcome evidence that the online conference had created a network of sufficient interest to maintain itself. Future online discussions should offer the option for participants to maintain contact as an online discussion group.

8. Effort should be made to persuade MPs to participate more actively in future online discussions. If technical training is needed to enable Members to access electronic discussions, this should be provided. Participation by MPs would help to break down the wall between 'public discussion' and 'parliamentary discussion'. Just as members of the public are participants alongside MPs in the many meetings that take place daily in and around Parliament, online discussions need to facilitate similar opportunities for ideas to be shared between representatives and the public, including those many citizens for whom visiting Westminster is very difficult.

OVERVIEW

The value of online discussion conferences, such as the one reported here, must be carefully researched. It is too early to make conclusive judgements about the success or failure of the exercise reported here, but this first experiment generated sufficient participation and interesting content to suggest that future online conferences would be worthwhile. The value of these discussions must be examined in distinction from other forms of online discussion, such as news groups, open fora and government-run consultations. The principal question to be considered in future experimentation should concern not just the value of online discussion as such, but the relevance of electronic discussions to parliamentary representation and a stronger model of deliberative democracy.

Dr Stephen Coleman,
Director of Studies,
The Hansard Society for Parliamentary Government
Melissa Simpson worked as research assistant on the compilation of this report.

November, 1998