House of Lords
House of Commons

Joint Committee on the Draft Communications Data Bill

Draft Communications Data Bill

Session 2012-13

Report, together with appendices and formal minutes

Ordered by the House of Lords and the House of Commons to be printed 28 November 2012

HL Paper 79
HC 479
Published on 11 December 2012
by authority of the House of Commons and the House of Lords
London: The Stationery Office Limited
£0.00

The Joint Committee on the Draft Communications Data Bill

The Joint Committee on the Draft Communications Data Bill was appointed by the House of Commons on 21 June 2012 and by the House of Lords on 28 June 2012 to examine the Draft Communications Data Bill and to report to both Houses by 30 November 2012. It has now completed its work.

Membership

HOUSE OF LORDS

Lord Armstrong of Ilminster (Crossbench)
Rt Hon Lord Blencathra (Chair) (Conservative)
Baroness Cohen of Pimlico (Labour)
Lord Faulks (Conservative)
Rt Hon Lord Jones (Labour)
Lord Strasburger (Liberal Democrat)

HOUSE OF COMMONS

Rt Hon Nicholas Brown MP (Labour)
Michael Ellis MP (Conservative)
Dr Julian Huppert MP (Liberal Democrat)
Stephen Mosley MP (Conservative)
Craig Whittaker MP (Conservative)
David Wright MP (Labour)

Powers

The Committee had the power to require the submission of written evidence and documents, to examine witnesses, to meet at any time (except when Parliament is prorogued or dissolved), to adjourn from place to place, to appoint specialist advisers, and to make Reports to both Houses. The Lords Committee had power to agree with the Commons in the appointment of a Chairman.

Publications

The Report of the Committee was published by The Stationery Office by Order of both Houses. All publications of the Committee (including press notices) are on the Internet at http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/.

Committee staff

The staff of the Committee were Chloe Mawson (Lords Clerk), Jessica Mulley (Commons Clerk), Michael Collon (Lords Second Clerk), Claire Morley (Committee Specialist), and Rob Dinsdale (Committee Assistant).

Contacts

All correspondence should be addressed to the Clerk of the Joint Committee on the Draft Communications Data Bill, House of Commons, 7 Millbank, London SW1A 0PW. The telephone number for general enquiries is 020 7219 8363; the Committee's email address is draftcommunicationsdatabill@parliament.uk

Contents

Report

Summary

It is the duty of Government to maintain the safety and security of citizens. This is not only in the public interest; it is in the interest of law-abiding members of the public. For this the law enforcement agencies must be given the tools they need. Reasonable access to some communications data is undoubtedly one of those tools. But the Government also have a duty to respect the right of citizens to go about their lawful activities, including their communications, without avoidable intrusions on their privacy. These duties have the potential to conflict.

More than a decade ago the Regulation of Investigatory Powers Act 2000—RIPA—set out the conditions which the law enforcement agencies and others have to satisfy if they wish to access communications data—the details about communications, but not their content. The Act specifies what data can be accessed, by whom, for what purposes, and subject to what conditions. Since 2000, however, methods of communicating have changed, and the volume of communications data potentially available to public authorities has increased very significantly. The draft Bill which we have been considering is the Government's endeavour to bring the law up to date.

We accept that there is a case for legislation which will provide the law enforcement agencies with some further access to communications data, but we believe that the draft Bill pays insufficient attention to the duty to respect the right to privacy, and goes much further than it need or should for the purpose of providing necessary and justifiable official access to communications data. Clause 1 would give the Secretary of State sweeping powers to issue secret notices to communications service providers (CSPs) requiring them to retain and disclose potentially limitless categories of data. We have been told that she has no intention of using the powers in this way. Our main recommendation is therefore that her powers should be limited to those categories of data for which a case can now be made. If in future a case can be made for the power to be increased, this should not be done without effective Parliamentary scrutiny. We recommend the procedure for this.

The same procedure should apply if the power to request communications data is to be given to more authorities than the police, intelligence and security services, SOCA, HMRC, FSA and UKBA. If data is required for wider purposes than at present, this needs primary legislation.

We believe that the current safeguards on the authorisation of applications for access to data are working better than is often thought, but we make recommendations for improving them, and for strengthening the roles of the Interception of Communications Commissioner and the Information Commissioner. We suggest amending the definition of "communications data" which no longer meets current needs. We have looked at jurisdictional problems which will face overseas network providers in particular. We criticise the Government's estimates of the cost of the Bill and the benefits to be derived from it; some of the figures are fanciful and misleading.

We believe our recommendations would result in a Bill which would give the law enforcement agencies the essential tools they need to tackle serious crime and terrorism but at the same time limit the risk of intrusion into the privacy of the vast majority of honest citizens.

1 History and Background

Historical background

1. There is nothing new about the use of communications data by the police and other law enforcement agencies and by the intelligence and security services. Since letters were sent and since the first records of telephone calls began to be kept, knowledge of who wrote or spoke to whom, when and how they wrote or spoke, and where they were when they did so—communications data—has been an important tool in the prevention, detection, investigation and prosecution of crime and of threats to the safety of the state. Knowledge of what people wrote or said—the content of communications—has also been valuable but, as we explain more fully later, that has been regulated entirely differently, and access to the content of communications is outside the scope of the legislation we are considering, It is not, however, beyond the scope of this report. As we explain in Chapter 5, though the distinction between communications data and content is theoretically clear, it may often be possible to draw from communications data inferences which give strong indications and which are evidentially acceptable of the probable nature and purposes of content. One of the more intractable problems we have had to consider is whether and if so how legislation can or should distinguish and proscribe access to data from which such inferences can convincingly be drawn.

2. During the last century there was virtually no statutory regulation or control of the persons who could obtain communications data and the uses to which it could be put except for the provisions of the Data Protection Acts 1984 and 1998 which dealt with the processing and protection of personal data, and some general information powers in various other Acts, which permitted a few public authorities to access documents.[1] Perhaps because postal and telecommunications services were originally provided by a state-owned monopoly (the Post Office), interception of all types (including access to communications data) was carried out under the Royal Prerogative with oversight by the Judges' Rules. The only practical limitation, from an investigator's perspective, was that it was not always easy for those wishing to access data to know if the data was there to be accessed, and if so, how to access it. They relied usually on the goodwill and cooperation of the telecommunications companies holding the data; short of a court order for the production of evidence, there were only limited powers to compel the companies to disclose whether they had any relevant data and, if they had, to disclose the data itself. Section 45 of the Telecommunications Act 1984 provided that the disclosure of communications data by a person running a public telecommunications system was *prima facie* an offence. It was, however, permissible to make a disclosure for the prevention or detection of crime or for the purposes of any criminal proceedings, in the interests of national security or in pursuance of a court order. Section 94 of the 1984 Act enables the Secretary of State to issue directions to telecommunications operators in the interests of national security.[2]

1 See further in paragraph 22.

2 We have been unable to obtain information about how section 94 of the Telecommunications Act 1984 has been used. The provisions of section 94 permit directions to be given without the need for them to be laid before Parliament if disclosure would be against the interests of national security. A person must not disclose anything done by virtue of section 94 if the Secretary of State has notified him that disclosure would be against the interests of national security.

3. In 2000 the Regulation of Investigatory Powers Act (RIPA) was passed. Chapter II of Part I of the Act—sections 21 to 25—for the first time attempted to regulate who could access communications data, what classes of data they could access, for what purposes, and subject to what controls. This chapter came into force on 5 January 2004[3] and is the principal law which currently governs access to communications data. The chapter does not regulate what data must be retained, dealing only with acquisition and disclosure. Importantly, the only data available to be accessed is the data retained by the Communication Service Providers (CSPs) for their own purposes. These provisions impose on them no obligation to retain data they do not need, or to retain it for longer than they need it. A voluntary Code of Practice was introduced in 2003 with telecommunications operators being asked to retain information on a voluntary basis on the understanding that they would be reimbursed for the additional costs incurred.

4. At the same time there were important developments on the European front. In April 2004 the United Kingdom was one of four Member States of the EU which put forward a proposal for the mandatory retention of data on communications networks for combating crime. This initiative was superseded in September 2005 by a Commission proposal for a Directive which would have the same effect. The United Kingdom then had the Presidency of the EU and, following the London bombings in July 2005, pressed ahead with the proposals. A general approach was agreed in December 2005, and the Directive was adopted on 15 March 2006.[4] This Data Retention Directive (DRD) had to be transposed into national law within 18 months, and the United Kingdom did so by Regulations which came into force on 1 October 2007.[5] These however applied only to fixed network and mobile phones; the Government postponed implementation with respect to "the retention of communications data relating to internet access, internet telephony and internet email". This was generally welcomed by providers, as the provisions relating to fixed network and mobile phones were far easier to implement than those relating to internet access, internet telephony and internet email.

5. In May 2008 the previous Government announced plans for legislation which would have required communications data to be stored for a year in a purpose-built database. The proposal would also have completed the implementation of the DRD in the United Kingdom. These plans were strongly criticised however, not least by the Information Commissioner. The Government withdrew the proposal, and instead completed the implementation of the DRD by new Regulations[6] which superseded and revoked the earlier Regulations. The 2009 Regulations are those now in force. They require CSPs notified by the Secretary of State to retain the categories of communications data specified in the Schedule for 12 months. Access to the data is governed by RIPA.

3 The Regulation of Investigatory Powers Act 2000 (Commencement No 3) Order 2003, SI 2003/3140, Article 2.

4 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105 of 13 April 2006, page 54. Even now, over five years after the date for transposition, not all Member States have implemented the Directive; in particular, the German Constitutional Court has ruled that the legislation implementing the Directive in Germany is unconstitutional.

5 The Data Retention (EC Directive) Regulations 2007, SI 2007/2199.

6 The Data Retention (EC Directive) Regulations 2009, SI 2009/859.

6. In April 2009 the Government put out to consultation a revised plan[7] in which they suggested that there were three possible approaches. The first was the previous proposal of a centralised database, which they said that they did not intend to pursue. The second was "doing nothing"; they said that they would be failing in their duty to protect the public if they "allowed the capability of public authorities to use communications data to degrade." Doing nothing was therefore in their view not an option. This, they said, left "a range of 'middle way' options" on which they were consulting. In fact only one option was put forward: legislation to compel CSPs based in the United Kingdom to collect and keep all data public authorities might need, including third party data crossing their networks, and to make all this data accessible on a case-by-case basis to public authorities "subject to the same rigorous safeguards that are now in place." An additional proposal—scarcely an alternative—was to address "the problem of fragmentation" by requiring CSPs not only to collect and store the data but to match third party data to their own data where it had features in common. The only choice for those who supported the middle way was therefore whether or not the compulsory retention and availability of data should be supplemented by requiring CSPs to process the data.

7. An analysis of the replies to this consultation paper was published six months later.[8] On the all-important question "Do you support the Government's approach to maintaining our capabilities? Which of the solutions should it adopt?" the Home Office said that 29% of respondents replied Yes, and 38% No—presumably to the first part of the question, since the second is hardly susceptible of a Yes or No answer. The Information Commissioner supported the approach on the basis that he was glad that the Government had abandoned the idea of a single database, but he remained concerned "that the case has yet to be made for the collection and processing of additional communications data for the population as a whole being relevant and not excessive". The Home Office cited this as him replying both "yes" and "no" to the same consultation question.

8. No legislation was proposed before the 2010 general election. The Coalition Agreement, published in May 2010, stated that "We will end the storage of internet and email records without good reason".[9] The Government took no action in the first session, but the 2012 Queen's Speech announced a draft Communications Data Bill. This was presented to both Houses on 14 June 2012.[10] This Joint Committee was constituted on 28 June 2012 with a remit to consider the draft Bill and report to both Houses by 30 November 2012.

The current position

9. The annual report of the Interception of Communications Commissioner (IoCC) for 2011 states that in that year 494,078 requests were made for access to communications data. We explain in the following chapter how this figure should be interpreted. On any view it is a major encroachment into individual privacy, but it is far from being the only one, and should be considered in context.

7 http://www.homeoffice.gov.uk/documents/cons-2009-communications-data?view=Binary

8 http://webarchive.nationalarchives.gov.uk/+/http:/www.homeoffice.gov.uk/documents/cons-2009-communication-data/cons-2009-comms-data-responses2835.pdf?view=Binary

9 "The Coalition: our programme for Government" , 10 May 2010, http://www.cabinetoffice.gov.uk/news/coalition-documents

10 Cm 8359.

BOX 1: Other examples of intrusion into individual privacy

Cheshire Constabulary estimated that in 2011 that there were 1.85 million CCTV cameras in the United Kingdom, 1.7 million of which were privately owned. The quality of the images has greatly improved.[11] In 2008 Transport for London alone had over 10,000 CCTV cameras on its rail network, and all its 8,000 buses have CCTV cameras.

The National Policing Improvement Agency operates a national DNA database, which is one of the world's largest, with profiles on an estimated 5,570,284 individuals as of 31 March 2012.[12] It also operates a national automated number plate recognition system, which by March 2011 was receiving 15 million sightings daily, with over 11 billion vehicle sightings stored.[13] In April 2010 the national fingerprint database contained the prints of 8.3m individuals.[14]

The ELMER database, kept by the Serious Organised Crime Agency (SOCA), includes over 1.5m suspicious activity reports submitted by banks, lawyers, insurance companies etc to combat money laundering.[15]

The National Pupil Database holds information on children in schools in England. It includes detailed information about pupils (pre-school, primary, secondary and further education), their test and exam results, prior attainment and progression for all state schools in England. Attainment data is also held for pupils and students in non-maintained special schools, sixth form and Further Education colleges and (where available) independent schools. The National Pupil Database includes information about the characteristics of pupils in the state sector and non-maintained special schools such as gender, ethnicity, first language, eligibility for free school meals, information about special educational needs, as well as detailed information about pupil absence and exclusions.

Mobile phones not only produce data relating to calls, short message service (SMS) messages and general packet radio service (GPRS) connections but they also leave a detailed trail of information relating to users' locations. CSPs know roughly which cell site each phone is connected to at any given time when the phone is switched on. They keep records of the actual cell sites used when communications are sent to and from the phone. This cell site may not be the site which is nearest to the phone, but it will be the site that sends the strongest signal to the phone. This location data can be used, when a phone is in constant use (for example if data is constantly being

11 See BBC research in 2009 on the density of local authority-owned cctv cameras: http://news.bbc.co.uk/1/hi/uk/8159141.stm and a Channel 4 News assessment that in 2008 there was a cctv camera for every 14 citizens. http://www.channel4.com/news/articles/society/factcheck+how+many+cctv+cameras/2291167.html

12 http://www.npia.police.uk/en/8934.htm

13 http://www.npia.police.uk/en/10505.htm

14 http://www.npia.police.uk/en/10504.htm

15 http://www.publications.parliament.uk/pa/ld201011/ldselect/ldeucom/82/82.pdf

"pushed" to the phone) to create a map of approximately where that phone was moment by moment. In areas saturated with cell sites this data can suggest locations to within a 50 metre radius. In sparsely populated areas, however, cell sites may connect with phones that are 25 kilometres away.

10. The reason for all this intrusion is not simply curiosity, or a desire by the authorities unreasonably to investigate individuals' private lives; though from many of the comments we have read this appears to be the view of a section of the public. The reason is that communications data is an invaluable weapon in the defence of national security and in the fight against crime—especially terrorism and other serious crimes. The intelligence and security services and the police are far and away the main users of communications data. There are not infrequently high profile cases where the importance of communications data to an investigation is clear to all.

BOX 2: Examples of the use of communications data in fighting terrorism and crime

In June 2007 a vehicle carrying improvised explosive devices was used in an attack on the main terminal building at Glasgow airport. Communications data was used to identify a bomb factory through analysis of calls from suspects' phones to a letting agency. Items and tools used in the making of devices were found, and forensic evidence tied the suspects to the premises. Communications data, including cell site analysis, identified where, from whom and when the vehicles involved were purchased. Communications data also provided evidence of contact between suspects and in particular identified the prior knowledge of a third party who was directed, via text, to an email account containing instructions detailing how that person should answer questions from the authorities after the event.

In 2002, during the investigation into the murder of Holly Wells and Jessica Chapman in Soham, communications data from their mobiles showed that they had been at or very close to the house of Ian Huntley, suggesting flaws in his alibi. Records of calls and text messages between Huntley and his ex-girlfriend, Maxine Carr, also showed that she was in Grimsby when Huntley killed the victims and that she deliberately misled the police over his whereabouts.

In August 2009 two men in disguises entered Graff Diamonds and stole £40m of jewellery. They left taking a hostage at gunpoint. Shots were fired in the street at those who gave chase. CCTV captured the suspects prior to entering the premises; this showed one using a mobile. A handset was recovered in an abandoned vehicle linked to the attack; from this other handsets were identified. Analytical work on call data established contact with the makeup artist who prepared the suspects' facial masks; a car hire firm used for getaway vehicles; and the locations of the suspects at various times during the robbery.[16]

16 This example is taken from the written evidence of the Metropolitan Police.

11. Less high profile, but no less important, is the use of communications data by Her Majesty's Revenue and Customs (HMRC) to uncover tax evasion. There are also uses of communications data which are not connected with crime, but where lives at risk can be saved: the location of individuals who are threatening suicide, and others in life-threatening situations. At the other extreme there are examples of the use of communications data, much quoted by those opposed to the legislation, which show what can happen if the system is misused or abused, and the safeguards are inadequate or bypassed. The majority of these relate to local authorities, and we deal with them in Chapter 4.

12. A special mention should be made of the work of the Child Exploitation and Online Protection Centre (CEOP), which uses communications data to detect paedophiles. Mr Davies, the Chief Executive, gave us a particularly startling example of how essential to their work was the ability to reconcile an Internet Protocol (IP) address to an individual.[17]

BOX 3: Reconciling an IP address to an individual

A child contacted a helpline service online, indicating that he had self-harmed and was intending to commit suicide. This was passed on to CEOP who acquired the communications data to reconcile the IP address to an individual. They did so in a very short space of time and passed it on to the local police force. When they got into the address the child had already hanged himself, but was still breathing. If there had been any delay, or if the child had been unlucky enough to be using one of those service providers that do not keep subscriber data relating to IP addresses, that child would now be dead.

13. "Exponential" is a word we have heard many times in the course of our inquiry but, as we explain in Chapter 3, it is barely adequate to describe the explosion in communications data over the decade since RIPA came into force. The changes in the forms of communications and the volume of exchanges are such that it is hardly surprising that the Government think it appropriate to amend the law governing access to communications data; and this is what the draft Bill would do.

Our procedure

14. We put out a call for written evidence, and in response received a great deal of valuable information and many conflicting views. All of this evidence is available on our website, except for two categories. The first of these is evidence which was sent to us in confidence. This has helped to inform us and to form our views, but we have not referred to it specifically in this report. The second category consists of some 19,000 emails we received from individuals in response to prompting from two organisations, 38 Degrees and the Open Rights Group. This reflects the anxiety felt by large sections of the public about intrusion by the authorities into their private lives.

15. In the course of five months, during two of which one or both Houses were in recess, we held 20 meetings (three of them while the House of Lords was in recess). We heard over

17 Q 1096

23 hours of oral evidence from 54 witnesses—in some cases more than once. These ranged from officials of the Home Office (the Bill's sponsoring department), the police and representatives of other law enforcement agencies, who strongly supported the Bill, to persons and bodies equally strongly opposed to it. The witnesses included the main United Kingdom CSPs and overseas based email providers and social networks. We concluded by hearing the Home Secretary, who spoke on behalf of the Government. Transcripts of all this evidence are available on our website, but in a few cases we allowed witnesses to give evidence to us in private so that the transcripts could be redacted before publication to remove matters that were commercially sensitive or which could have compromised security. Where redactions have been made, this appears in the transcript. To all our witnesses we are most grateful.

16. We went on two visits. The first was to the Metropolitan Police Central Intelligence Unit (CIU); the second to Everything Everywhere, the company which owns and operates both the T-Mobile and the Orange networks. We include notes of those visits in Appendices 4 and 5. Of particular value to us was to see in operation the procedure by which the authorities request communications data from CSPs, and the procedure of CSPs in response to those requests. We are grateful to both organisations for their time and trouble.

17. We asked to see the intelligence service, the security service and GCHQ. Their views on the draft Bill would have been helpful to us. The Home Secretary, in accordance with usual practice, would not permit them to give evidence to us, even in private. She offered us "a general briefing on the threat, particularly that from international terrorism, and the Security Service's role in addressing it, [which] would take place off the Parliamentary estate and would be strictly informal and off-the-record". We did not see that this would advance our scrutiny of the draft Bill, and declined the invitation. The intelligence and security services did however give evidence to the Intelligence and Security Committee. This, like us, is a Committee of members of both Houses of Parliament, but it is not a Parliamentary Committee and reports to the Prime Minister rather than to Parliament. Its inquiry into the draft Bill has been limited to the needs of the intelligence and security services. The conclusions and recommendations of the Intelligence and Security Committee are being published on the same day as this report. We thank the Committee for giving us advance sight of its recommendations.

18. We also wish to place on record our thanks to our specialist adviser, Mr Martin Hoskins, for the support he provided during our consideration of the draft Bill.

19. Pre-legislative scrutiny provides the opportunity for members from all sides of both Houses to come together and scrutinise the principle and the detail of potentially sensitive draft legislation. It gives an opportunity to build both Member expertise and political consensus. It allows interested parties from outside Parliament to engage with Parliament's scrutiny process and to help inform Members on the consequences of implementing the proposals. It gives Government the chance to hear the preliminary views of Parliament at a stage when policy can still be amended before the introduction of a Bill proper.

20. **We welcome the Government's decision to publish this Bill in draft form. We hope that Departments from across Government will continue to show a commitment to publishing as much legislation as possible in draft, and that Parliament will continue to take advantage of the opportunities that exist for pre-legislative scrutiny.**

2 What RIPA does, and how the system currently functions

21. Chapter II of Part I of RIPA essentially deals with four matters:

- what categories of communications data should be available;
- who can access it;
- for what purposes; and
- subject to what safeguards.

22. As we have said, the annual report of the IoCC for 2011 states that in that year 494,078 requests were made for access to communications data. The great majority were made under RIPA, though there are a number of other statutory information-gathering powers which can be used by public authorities to acquire communications data. Clause 24 of and Schedule 2 to the draft Bill will amend certain powers in other legislation so that they may not be used in the future to oblige CSPs to disclose communications data. This is intended to consolidate the powers under which communications data can be disclosed.

BOX 4: Requests, crimes and individuals

There is a difference between the numbers of requests, the numbers of people being investigated, and the numbers of crimes being investigated. Many requests may be made in relation to the same person because that person may use a large number of devices (criminals habitually change 'phones on a regular basis to try to evade detection); conversely one request can reveal data on many people. Nor does the number of requests equate to the number of crimes investigated. Many requests can be made during an investigation into a single crime; a significant murder, organised crime or counter-terrorism investigation can involve hundreds of communications data requests.

Data that can be accessed

23. Data can of course only be accessed if it is available. CSPs are commercial organisations; they generate data only if it is useful and they keep it only for as long as it is necessary, but storage is expensive, and once they no longer have a business purpose for data, they will delete it unless they are required to retain it under the Regulations implementing the Data Retention Directive. Otherwise they are currently under no duty to preserve data, nor will they do so. One of the main drivers of the legislation is to give the Government the power to require CSPs to generate and retain data for which they have no business purpose.

24. When RIPA was enacted communications were still mainly by post or by phone, though emails were gaining in popularity, and the distinction between communications data and content was relatively straightforward. In the case of post, communications data was what was written on the outside of the item, and the rest was content. Phone calls were

calls between landlines, between mobile phones, or between landlines and mobile phones. Communications data is therefore defined in RIPA as three elements:

- traffic data (essentially, data identifying the location of the device to or from which the communication is sent, the equipment through which it is transmitted and the signals actuating equipment);
- use data (data, other than content, about the use made of a service); and
- subscriber data (data held by the service provider about the persons to whom it provides the service, other than traffic data or use data).

Accessed by whom?

25. Section 25(1) of RIPA as originally enacted listed six public authorities permitted to access communications data. These included, in addition to police forces and the intelligence and security services, the National Criminal Intelligence Service and the National Crime Squad, which are now superseded by SOCA,[18] and the Commissioners of Customs and Excise and Commissioners of Inland Revenue, now superseded by HMRC.[19]

26. In addition, the Secretary of State has power by order to add any public authority. Over the years a large number of authorities have been added in this way.[20] For some, like the Financial Services Authority (FSA), a good case can be made. The inclusion of all local authorities is more controversial; the inclusion of some others seems hard to justify, even though they can access communications data only for limited purposes. In Chapter 4 we give our views on which authorities should appear on the face of the draft Bill, and the procedure which should be followed for any amendments to this list.

Permitted purposes

27. RIPA, as originally enacted, provided that communications data could be obtained only if to do so was "necessary" on one of the following grounds:[21]

> " (a) in the interests of national security;
> (b) for the purpose of preventing or detecting crime or of preventing disorder;
> (c) in the interests of the economic well-being of the United Kingdom;
> (d) in the interests of public safety;
> (e) for the purpose of protecting public health;

18 Paragraph 135 of Schedule 4 to the Serious Organised Crime and Police Act 2005 makes amendments to section 25 of RIPA consequential to this change. The Scottish equivalent, the Scottish Crime and Drug Enforcement Agency (SCDEA), was added by paragraph 4(5) of the Schedule to the Police, Public Order and Criminal Justice (Scotland) Act 2006 (Consequential Provisions and Modifications) Order 2007, SI 2007/1098.

19 Paragraph 8 of Schedule 12 to the Serious Crime Act 2007 makes the consequential amendment to section 25 of RIPA.

20 The Regulation of Investigatory Powers (Communications Data) Order 2010, SI 2010/480, lists all the relevant public authorities, and gives the ranks of the persons designated to grant access to communications data and the purposes for which they may grant authorisations.

21 Section 22(2)

(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

(g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health."

28. There was also a power for the Secretary of State to add, by order subject to affirmative resolution, "any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State". Two additions have been made under this power:[22]

" (a) to assist investigations into alleged miscarriages of justice; and

(b) where a person ("P") has died or is unable to identify themselves because of a physical or mental condition—

(i) to assist in identifying P, or

(ii) to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition."

These are currently the nine permitted purposes. If communications data is not "necessary" for one of these very broad purposes, it cannot be accessed under RIPA.

The safeguards under RIPA

29. Any of many thousands of police officers may think that communications data is necessary to help them with a criminal investigation. Authorisation therefore has to be given by Designated Senior Officers independent of the inquiry. Designated Senior Officers are trained in considering the impact of necessity, proportionality and collateral intrusion on an individual's privacy. Before an application reaches the Designated Senior Officer, it is channelled through a Single Point of Contact (SPoC). The SPoC is an officer who has undergone formal training, is independent from the investigation, will advise the applicant, and will submit applications for authorisation if, and only if, they meet all the formal requirements, including those of necessity and proportionality. Authorisation is then given by the Designated Senior Officer, also independent from the investigation. If the application is authorised, it is returned to the SPoC officer who will obtain the communications data from the CSP and pass it to the applicant.

30. The seniority of the officer granting the authorisation is prescribed by an order made by the Secretary of State.[23] In the police forces no officer under the rank of Superintendent can authorise an application for all classes of communications data, though Inspectors can authorise applications for subscriber data. The purposes for which authorisations can be granted are also limited; the police can grant authorisations for all purposes except tax assessment and collection, and the investigation of possible miscarriages of justice, while

22 by the Regulation of Investigatory Powers (Communications Data) (Additional Functions and Amendment) Order 2006, SI 2006/1878, which is now consolidated by the Regulation of Investigatory Powers (Communications Data) Order 2010, SI 2010/480.

23 RIPA, section 25(2)-(5)

only HMRC can grant authorisations for tax purposes, and authorisations for investigations into miscarriages of justice can be given only to the Criminal Cases Review Commission and its Scottish equivalent. Fire Control Officers and Control Supervisors in Ambulance Control Rooms can access all communications data, but for the single purpose of dealing with death or injury in an emergency. If they wish to access communications data for preventing or detecting crime, authorisation is needed at a more senior level, and will not extend to traffic data.

31. Some witnesses suggested to us that the authorisation system was simply a means of rubber-stamping applications.[24] We are satisfied that this is not the case and we explain why in Chapter 5.

32. An additional safeguard was the creation by section 57 of RIPA of the office of IoCC, one of whose duties is "to keep under review … the exercise and performance, by the persons on whom they are conferred or imposed, of the powers and duties conferred or imposed by or under Chapter II of Part I [of RIPA]". In other words, he inspects the working of the system for access to communications data to make sure that it is done entirely in accordance with the statute, and makes recommendations for improvement when errors occur. The purpose is to reassure the public that intrusion is kept to a minimum and their privacy is respected as far as is consistent with the aims of the legislation. Whether this reassurance is achieved is again something we consider in Chapter 5.

Communications data held overseas

33. RIPA is drafted so as to attempt to give United Kingdom public authorities a legal basis for requesting communications data from CSPs based overseas if they operate a service in the United Kingdom. However, many overseas CSPs refuse to acknowledge the extra-territorial application of RIPA. The procedure can of course be used to request access to data, and many CSPs will comply but emphasise that they are doing so on a voluntary basis; others will refuse to respond to RIPA requests at all. At that stage the only way in which United Kingdom law enforcement authorities can access the data is through the arrangements for international mutual legal assistance which allow the judicial and prosecuting authorities of one state to seek from the authorities of another state help in the prevention, detection and prosecution of crime. We consider these arrangements in Chapter 6.

24 E.g. David Davis MP and Dr Gus Hosein, Q 118

3 Is there a need to access more communications data?

The 25% missing data figure

34. The Government assert that the powers contained in the draft Bill are necessary to ensure that the powers of law enforcement, national security agencies and other public authorities keep pace with technological change. Communications technologies and services are constantly evolving and the Government are concerned that "the ability of the police and others to use this vital tool is disappearing because communications data from new technologies is less available and often harder to access".[25] The Government state that at present approximately 25% of communications data required by investigators is unavailable and that without intervention this will increase to 35% within two years.[26] The aim of the Bill is to bring availability back to around 85% by 2018.[27]

35. The 25% figure has been much quoted in aid of the draft Bill but has also attracted considerable criticism. It is not clear what methodology was used to arrive at the 25% figure. The Internet Service Providers' Association (ISPA) questioned how the baseline of 100% of data had been derived,[28] and we agree that this is not clear. We understand that the figure is based on research commissioned by the Home Office in 2011 on changing public use of communications combined with an appraisal of the technical feasibility of various methods to obtain communications data from CSPs but the Government did not share the details of either of these projects with us. It is not a simple case of being able to measure the percentage of requests for communications data which are turned down by CSPs because the figure includes requests that would have been made but were not made because the SPoCs knew the data would not be available so did not take the request forward.

36. We are of the strong view that the 25% data gap is an unhelpful and potentially misleading figure. There has not been a 25% degradation in the overall quantity of communications data available; in fact quite the opposite. Technological advances and mass uptake of internet services since RIPA was passed in 2000, including social networking sites, means that there has been, and will continue to be, a huge increase in the overall amount of communications data which is generated and is potentially available to public authorities. This is illustrated in Box 5.

BOX 5: Increase in the volume of communications data since 2000

In 2000, just half of UK adults said that they had a mobile phone—that figure now stands at 92%. There are now 81.6 million mobile subscriptions in the United Kingdom.[29]

25 Home Office Q&A brief, page 10

26 Home Office written evidence, paragraphss 13 and 15

27 Home Office written evidence, paragraph 16

28 ISPA written evidence, paragraph 23

29 http://www.mobilemastinfo.com/stats-and-facts/

August 2001 was the first month in which over one billion text messages were sent in the United Kingdom.[30] Over 150 billion text messages were sent in 2011.[31]

Mobile subscribers only began to access the internet when GPRS technologies were introduced in 2002. Take up was slow, as it took time for providers to develop services (such as picture messaging and web browsing) that could easily be used, and for customers to be encouraged to buy internet-enabled devices.

The maximum speed of a mobile data connection offered in 2003 was about 32–40 kbit/s.[32] By December 2010, in good 3G coverage areas, average mobile speeds were 2.1Mbit/s.[33] With the advent of 4G, these mobile broadband speeds will increase very significantly.[34] This compares with the average fixed broadband speed of 6.2Mbit/s (November/December 2010).[35]

Social networking sites were in their infancy in 2000. MySpace was launched in 2003. Facebook was not launched until 2004.[36] It had a million users by the end of 2004, 100 million users by August 2008 and 1.01 billion globally by September 2012.[37] There are 30 million active Facebook users in the United Kingdom, around half of whom log on every day. Twitter was launched in July 2006.[38] It took 3 years 2 months for the billionth tweet to be sent. Now a billion tweets are sent every 2.5 days.[39]

In 2012, over 5.1 million customers access mobile broadband services via a laptop and dongle, and 39% of UK adults use their mobile phones to access the internet. The average UK consumer spends 90 minutes per week accessing social networking sites and e-mail, or using a mobile to access the internet, while for the first time ever time spent on calls on both fixed and mobile phones has declined.[40]

The total number of United Kingdom fixed broadband connections passed 20 million for the first time in 2011. In addition, the number of mobile broadband connections passed 5 million during the year, and by the first quarter of 2012 76% of United Kingdom homes had a broadband connection.[41]

30 http://www.text.it/mediacentre/facts_figures.cfm

31 http://stakeholders.ofcom.org.uk/market-data-research/market-data/communications-market-reports/cmr12/uk/?pageNum=7

32 http://en.wikipedia.org/wiki/GPRS

33 http://media.ofcom.org.uk/2011/05/26/mobile-broadband-speeds-revealed/

34 http://www.telegraph.co.uk/technology/news/9533158/iPhone-5-Britains-first-4G-mobile-network-hopes-for-exclusivity.html

35 http://media.ofcom.org.uk/2011/05/26/mobile-broadband-speeds-revealed/

36 http://en.wikipedia.org/wiki/Facebook

37 http://finance.yahoo.com/news/number-active-users-facebook-over-years-214600186--finance.html

38 http://en.wikipedia.org/wiki/Twitter

39 Evidence of Colin Crowell, Head of Global Public Policy, Twitter, Q 654.

40 http://stakeholders.ofcom.org.uk/market-data-research/market-data/communications-market-reports/cmr12/uk/?pageNum=7

41 http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/CMR_UK_2012.pdf p14

37. As the London Internet Exchange (LINX) put it:

> "Certainly, as people make ever greater use of Internet-based services, there is an ever greater quantity of data that either exists, or could be brought into existence by statutory requirement. However to say that this "is no longer always retained by communications providers" is highly misleading: communications providers are retaining more communications data than ever before and making it available to public authorities under existing law. The mere fact that even more data could be created, collected and made available hardly constitutes a loss."[42]

38. It is true that that even if there is more communications data available than ever before there may still be an operationally significant gap. Bob Hughes, Government Programme Manager, Telefónica UK–02, made the point that technology is constantly moving on and changing what is available and what is not.[43] Charles Farr confirmed that this was the problem the legislation seeks to address: "...there are far more communications and data attached to them, and there is far more data generally crossing the internet, not all of which is about communications. Those three things are definitely true. The key point is that the data there does not enable us to address the questions that law enforcement and the agencies have to address; in other words, there is more data but it is not always relevant or useful to us".[44]

39. **It is acknowledged on all sides that the volume of communications data now available is vastly greater than what was available when RIPA was passed. The much quoted figure of a 25% communications data gap purports to relate to data which might in theory be available, but currently is not. The 25% figure is, no doubt unintentionally, both misleading and unhelpful.**

The missing data elements

40. It was not long into our inquiry that we began to question the utility of the 25% figure and we asked the Home Office to identify what specific data types are currently missing. After some months the Government agreed to tell us on a confidential basis that there were three main data types that they hoped the legislation would be used to make available. At that point they argued that these data types could not be publicly identified without risking exposing loop holes to criminals. This need for secrecy was one of the drivers for the very broad drafting of clause 1.

41. Finally, on 24 October Home Office officials publicly identified the data types that are frequently not available and that the Government intend to secure through the legislation. These are: (i) subscriber data relating to IP addresses (i.e. who is using an IP address at any given point); (ii) data identifying which services or websites are used on the internet (i.e. the web address up to the first /); (iii) data from CSPs based overseas who provide webmail and social networks to users in the United Kingdom.[45]

42 LINX written evidence, paragraph 36.

43 Q 443 & 445

44 Q 874

45 Q 865

42. **We accept that IP addresses and web logs and data generated for business purposes but not retained by overseas CSPs are three data types which the law enforcement and other agencies cannot always access. We discuss in this report whether access to these data categories is necessary and, if it is to be enabled, the additional safeguards which will need to be introduced.**

The capability gap

43. It is not the case that these three data types account for the entire gap. Part of the gap is down to a lack of ability on behalf of law enforcement agencies to make effective use of the data that is available. This was confirmed in evidence from senior police officers including Sir Peter Fahy, the Chief Constable of Greater Manchester Police.[46] Detective Superintendent Steve Higgins from the National Police Improvement Agency explained:

> "Are the police equipped and do they have sufficient knowledge? In April 2010, we conducted a national training needs analysis to look at just this very issue; we identified a number of skills gaps, not just in relation to accredited SPoCS but also in relation to investigators and analysts, in particular".[47]

44. He then went on to explain that the National Police Improvement Agency has tried to address this through new courses for SPoCs, investigators and analysts. The accreditation of SPoCs is currently being reviewed and a programme of continuing professional development is being implemented. The National Police Improvement Agency is also looking to embed training on communications data within existing programmes of training for detectives.[48]

45. **Part of the gap is down to a lack of ability on behalf of law enforcement agencies to make effective use of the data that is available. Addressing this should be a priority. It does not require fresh legislation but will involve additional expenditure.**

46 Q 1095

47 Q 1108

48 Ibid.

4 What would the draft Bill change?

Failure to consult

46. The draft Bill would replace Chapter II of Part I of RIPA, and also other statutory provisions about access to communications data, with a new statutory regime making important, controversial and far-reaching changes which would potentially affect anyone who communicates by electronic means or who accesses the internet. It would particularly affect the CSPs. It was therefore unquestionably a prime candidate for wide-ranging consultation at a stage when policy was still being formulated and could be amended. This did not happen.

47. The draft Bill could impose substantial obligations on all major CSPs operating in the United Kingdom, potentially involving them in re-structuring of their systems, and certainly requiring a substantial commitment of human, financial and technical resources. Since they are to be allowed to recoup their expenditure from the public purse, it would have been to their advantage and to the taxpayer's if the policy could have been formulated to allow the greatest benefits for the least expenditure.

48. In the course of three evidence sessions we took evidence from 12 witnesses from the major United Kingdom CSPs: BT, Virgin, Vodafone, Everything Everywhere, Telefónica (O2); and several of the major overseas CSPs: Google, Hotmail, Yahoo!, Facebook, Twitter, and Skype. The evidence we received from the first five of these was to the effect that they had meetings with Home Office officials, sometimes frequent and usually at a high level, to discuss communications data, but that none of these dealt specifically with policy formulation; some were before the draft Bill was published (but not long before), and some were post-publication. The evidence of Mark Hughes for Vodafone was typical: "We have regular meetings with the Home Office at a high level. We have had one meeting with the Home Office, formally, post the drafting of the Bill, where we had the opportunity to ask questions. Some of the questions they were not able to answer for reasons of sensitivity." [49]

49. The position of the overseas based email service providers was worse, with the first contact from the Home Office often coming after they first heard that we had invited these companies to give us oral evidence. Emma Ascroft told us on behalf of Yahoo!: "We were invited after the Home Office heard that we had been invited to give evidence to this Committee …. We had had no contact before. We met the Home Office in March 2011 to discuss the Government's response to the 2009 consultation on the changing communications environment, which Yahoo! UK responded to. We asked for a meeting in September, at which point the Home Office said there was no progress to report…. there was no further contact. As I said, the meeting we had with the Home Office was three weeks ago. Again, it was very much presented to us as our opportunity to ask the Home Office questions. It was not for the Home Office to consult us on any options."[50] This too was the position of the social network providers. On behalf of Facebook, Simon Milner said categorically: "We had no dialogue with the Home Office before the Bill was published ...

49 Q 421. See also the replies of Simon McCready (Virgin) (Q419), Jonathan Grayling (Everything Everywhere) (Q421), Bob Hughes (Telefónica/O2) (Q422), and Mark Hughes (BT) (Q423).

50 QQ 548-549 See also the evidence of Stephen Collins (Hotmail) and Sarah Hunter (Google) (Q547).

we were never asked [for input] and we never provided it." Similarly, Colin Crowell for Twitter: "We had one conversation with the Home Office about two and a half weeks ago.[51] So we, too, were contacted after the Bill had been published and had one phone conversation with them about it."[52]

50. We asked Charles Farr about this apparent lack of consultation. In the case of the United Kingdom CSPs he said: "We have been meeting regularly with UK CSPs on communications data over the past few years, and certainly in the run-up to the Bill. I believe that we shared our broad thinking about what we had in mind before the Bill was published, and we have followed that up with more detailed sessions since the Bill appeared ... but I fully accept that those discussions need to continue and go into more detail as we get closer to the time when the Bill is enacted, should it be so."[53]

51. In the case of the overseas providers, Mr Farr told us that he had read their evidence "with a lot of interest"; what he told us was almost the opposite of what they said. He asserted that there had been a total of 30 meetings with them over a two-year period. He conceded that, because they went back two years, not all of the meetings were on "the minutiae of the Bill", but all of them were on communications data.[54] On the face of it, there is an inconsistency between these two accounts. But our witnesses from the CSPs assumed, correctly, that a Committee inquiring into a draft Bill would be asking about meetings specifically on that Bill.

52. We asked the Home Office for details of the meetings they had had with Everything Everywhere. They sent us a list of 22 meetings which had been held since May 2009. The last five took place after publication of the Bill. Of the other 17, 12 were described as "Forum with key CSPs", the other five as bilateral with EE. One of these was with James Brokenshire MP, the Parliamentary Under-Secretary of State responsible for security. Officials explained that many of these meetings were wider working group meetings at which communications data was discussed "so that they [EE] may not recognise them all as specific Bill meetings". When we put the list to Jonathan Grayling, the Head of Law Enforcement Liaison at Everything Everywhere who had given evidence to us, he confirmed that these meetings did indeed form part of a series of regular meetings with the Home Office at which they discussed communications data matters generally and any outstanding problems. While he valued these meetings, at some of them the draft Bill was only an agenda item, usually consisting of a legislation update detailing timescales and high level plans; the meetings did not involve the Home Office asking for input to the detailed policy and content of the draft Bill. The meeting with the Minister on 17 November 2011 (also attended by James Blendis, Legal Vice President, Everything Everywhere) was the first at which the Bill was discussed; this was at a very high level, without going into any detail. The first meeting Mr Grayling described as specifically on the draft Bill was on 2 April 2012 (a meeting not on the Home Office list). This of course was only a month before the Queen's Speech, and two months before publication of the draft Bill. Industry was first given sight of the draft Bill, under embargo, on 7 June 2012, the week before its publication; this was the first indication they had of how the Bill was drafted.

51 This evidence was given on 6 September.

52 QQ 603-608

53 QQ 841-847

54 QQ 841-842

53. What is absolutely clear to us is that the regular meetings with EE and the other major CSPs would have been an unrivalled opportunity for the Home Office to discuss with them the evolving policy and content of the Bill, and to seek their input on the many matters where their technical and general expertise could have made a valuable contribution; and that this opportunity was not taken. The draft Bill is the poorer for it.

54. Mr Grayling has told us: "Subsequent to the publication of the Bill, consultation has increased dramatically, and we have had a number of useful meetings at the Home Office (documented in their list) and they have asked us to provide input into the way the Bill is drafted and any wording/clause amendments that we feel would be beneficial." We are glad to hear this; but, of course, the consultation would have been a great deal more valuable eighteen months ago.

55. Mr Farr told us: "Parliament and others had a right to see the legislation before we discussed it in detail with overseas providers."[55] We do not accept this. Parliament has a right to see, on its introduction, a Bill which seeks to implement as fully and clearly as possible the Government's policy, however controversial that policy may be. If the policy depends to a large extent on whether it can be implemented by a few major international corporations, not to consult them in the formulation of the detailed policy seems unwise. We note that the Intelligence and Security Committee has come to a similar conclusion.

56. **The Home Office should not have assumed that a consultation paper published in April 2009 could justify publication of draft legislation three years later without further consultation with the public and with those most closely affected by its proposals.**

57. **The evidence we received shows that United Kingdom CSPs were not given any details about the possible content of notices before the draft Bill was published, overseas CSPs were not consulted about the draft Bill at all, nor was there any further public consultation.**

58. **Before re-drafted legislation is introduced there should be a new round of consultation with technical experts, industry, law enforcement bodies, public authorities and civil liberties groups. This consultation should be on the basis of the narrower, more clearly defined set of proposals on definitions, narrower clause 1 powers and stronger safeguards which are recommended in this report. The United Kingdom and overseas CSPs should be given a clear understanding of the exact nature of the gap which the draft Bill aims to address so that those companies can be clear about why the legislation is necessary.**

59. **Even though many of them are prepared to cooperate on a voluntary basis, they should also be told what obligations might be imposed on them. For many, their willingness to cooperate voluntarily will be reinforced if there is a statutory basis for the requirement.**

60. **Meaningful consultation can take place only once there is clarity as to the real aims of the Home Office, and clarity as to the expected use of the powers under the Bill. CSPs should be consulted on the basis of drafts of the specific notices which will be served on them; these will have the detail of the obligations to be imposed on them, and enable**

55 QQ 843

them to undertake a better assessment of feasibility and of the resources and timescales involved.

Clause 1: What communications data would be accessible?

The breadth of clause 1

61. The provision at the centre of the draft Bill, on which all else depends, is clause 1. This is headed "Power to ensure or facilitate availability of data". It allows the Secretary of State by order to ensure that communications data is available from telecommunications operators so that it can be obtained by public authorities. The clause then sets out the main ways in which it is expected that the power will be exercised. The Home Office states[56] that in practice an order is likely to impose requirements on operators to generate all "necessary" communications data for the services or systems they provide; to collect "necessary" communications data, where such data is available but not retained; to retain the data safely and securely; to process the retained data to facilitate the efficient and effective obtaining of the data by public authorities; and other matters.

62. These are wide, general requirements which will be contained in an order. We have not seen a draft of such an order, and we have been told that we will not be shown one. But it is clear that the order will only be a framework. The specific requirements will be imposed by secret notices by the Secretary of State. The explanatory notes published with the draft Bill explain: "The expectation is that notices will therefore be individually tailored to each system or service (or class of system or service) in respect of which there is an operational need for communications data to be available from an operator. The notices will describe, by reference to each service and system, the description of data which must be retained, where the data should be stored and, if necessary, how the data should be collected, generated and processed."

63. A number of points stand out. First, the only limitation on what communications data should be made available is that it should be "necessary". Who decides what is "necessary", and for what purpose, is not specified; but as the word appears in the explanatory notes and not in the clause itself, it provides no reassurance. Secondly, even if we were able to see a draft order, it would be of limited assistance, since the requirements themselves will be in notices agreed between the Home Office and each relevant operator or, if not agreed, imposed on them. Parliament will not even see, still less have any control over, such notices. Thirdly, for the first time the CSPs may have to generate data which they would otherwise not have generated because there was no commercial need to do so. This data must be retained for 12 months—longer if it is required for legal proceedings—and will be available to the public authorities listed in the draft Bill or added to that list by order, for the purposes specified in the Bill, and subject to the safeguards in the Bill.

64. The power of the Secretary of State under clause 1 has thus been made as wide as possible— deliberately so, for the reasons we explain later. But the Home Office told some of the CSPs that they had no intention of exercising the powers widely, as Sarah Hunter explained on behalf of Google: "...the intent behind the Bill of the officials we met seemed

56 In the Explanatory Notes to the draft Bill

to be very narrow and reasonable. When we pointed out that the powers within the Bill were much broader than that, they could not quite address why there was such a gap."[57]

65. The Home Office told us almost from the outset of our inquiry that they had no need to issue notices extending to a wide range of data, and no intention of doing so; but, as explained in Chapter 3, they would not tell us publicly what the gaps were which the notices would be used to fill, because they did not want to publicise what data they currently cannot access. They accordingly made this clear only in a confidential annex to their written evidence. Subsequently however, in the second public evidence session with Home Office officials, Richard Alcock said:[58] "We have had discussions [with CSPs] about the additional data types that we may wish those service providers to retain … there is certain information which is not stored routinely by UK CSPs, in some cases web logs and in some cases IP data ... In the majority of cases, fundamentally it is about those two issues, but there is a broad range of other aspects." Charles Farr endorsed this: "As Richard has said, one of the areas where we are struggling is IP resolution. It is not the only area; the web log issue is also important."[59] Subsequently Charles Farr repeated this again, adding that there was also the issue of third party data which needed to be addressed.[60]

66. We address later in the chapter the vexed issue of whether these data types are all essential. Given the wide anxiety raised by the breadth of clause 1, we pressed the Home Office officials as to why it could not be narrowed to cover only the gaps which currently needed to be filled. Mr Farr's answer was: "The fundamental reason why we are nervous about limiting clause 1 is future-proofing ... Because I genuinely believe that no sooner will you get this legislation through than something else will come up, given the pace of change in the communications industry, which will create another gap, particularly if clever people know that we have filled one area, and so now try to exploit another. Future-proofing and flexibility are at the heart of the language we have used in clause 1." He accepted that the Home Office could and should look again at the drafting of clause 1: "I still come back to the point that we can look again at clause 1 and still have future proofing, because I think we need to emphasise more clearly that the data types we are interested in are only those which are relevant to these core questions." We did receive from Mr Farr the important undertaking that Home Office officials would look at clause 1 again, and advise Ministers on whether it can be changed, enhanced or improved."[61] We believe that it can indeed be changed and improved, by being narrowed to cover specifically the gaps so far identified. An undertaking, whether by officials or by ministers, that a power will be used only to a limited extent, is of little value. Once a power is on the statute book, it is available to be used, and also to be misused or abused, at any time in the future. It is hardly surprising that a proposal for powers of this width has caused public anxiety.

67. We accept that, given the rapidity of technological change and development in IT, within a relatively short time after the implementation of any legislation the Secretary of State may need to be able to order the retention of other categories of data. We accept too that changes may need to be made from time to time for other reasons. Neither of these

57 Q 553

58 Q 865

59 Q 869

60 Q 919

61 Q 869

justifies the retention of clause 1 in its current form. We note that the Intelligence and Security Committee has come to a similar conclusion and has recommended that: "more thought is given to the level of detail that is included in the Bill, in particular in relation to the Order-making power. Whilst the Bill does need to be future-proofed to a certain extent, and we accept that it must not reveal operational capability, serious consideration must be given as to whether there is any room for manoeuvre on this point: Parliament and the public will require more information if they are to be convinced."

68. We attach in Appendix 7 a note considering which Parliamentary procedures might be appropriate for making such changes while still retaining Parliamentary control and public confidence. Primary legislation should not in our view be ruled out; even without having resort to emergency legislation, a department like the Home Office with Bills every session should not have much difficulty in securing any necessary changes within a relatively short time. We can however understand the reluctance of ministers to be obliged to have frequent resort to primary legislation. Our recommendation is therefore for an order subject to the super-affirmative procedure we describe in Appendix 7, allowing full consideration by Parliamentary Committees. We caution however that this should not necessarily be assumed to be always a speedier process than primary legislation. Where the case for change can be made out, Parliament will have a duty to attempt to expedite the Parliamentary process, but even so, primary legislation could sometimes be faster. Of course, the inclusion of an order-making power would not preclude the Secretary of State from making use of primary legislation if an appropriate opportunity were to arise.

69. **The Home Office was able to tell us of specific types of data that are currently not routinely retained for business purposes by United Kingdom (and many overseas) CSPs and which would be useful to law enforcement and other investigations. It is the Home Office's intention to issue notices under the Bill to ensure that an unknown number of CSPs retain these specific types of data. The Home Office has however made clear to us that it does not currently need the power under this legislation to require other types of data be retained, and does not for the present intend to issue notices going more widely (except to CSPs which are not covered by the EU Data Retention Directive, which might be asked under this legislation to retain for 12 months data which they already create for business purposes). Clause 1 therefore should be re-drafted with a much narrower scope, so that the Secretary of State may make orders subject to Parliamentary approval enabling her to issue notices only to address specific data gaps as need arises.**

70. **The Home Office has argued that there is a case for keeping clause 1 wide because there may be other data types that emerge from time to time which will be important to law enforcement but will not be routinely retained by CSPs for business purposes. We do not accept that this is a good reason to grant the Secretary of State such wide powers now. We do not think that Parliament should grant powers that are required only on the precautionary principle. There should be a current and pressing need for them.**

71. **We do however accept that, depending on how the communications world develops, the Home Office may in future need the power to require the retention of other data types. Parliament and government both need to accept that legislation that covers the internet and other modern technologies may need revisiting and updating regularly. We have considered how the Secretary of State might be given powers in the future to**

allow her to address new and significant data gaps if and when they emerge. The alternatives seem to be either primary legislation on each occasion, or a power to amend clause 1 by order subject to a super-affirmative procedure which would guarantee fuller Parliamentary consideration than a standard affirmative order.

72. **We attach in Appendix 7 a consideration of the relative advantages and disadvantages of each course. On balance our preference is for an order subject to the super-affirmative procedure. We recognise that this will impose obligations on Parliament which it will have a duty to discharge effectively.**

IP address resolution and web logs

73. As outlined in paragraph 65, Home Office officials eventually told us in public evidence that they would like clause 1 to enable them to access two specific types of data: subscriber data relating to IP addresses and web logs.

74. Subscriber data relating to IP addresses is the information that makes it possible to trace who is using an IP address at a given point in time. An IP address is a numerical label assigned to a device connected to the internet (e.g. a computer, smart phone or printer). The IP address of a device is not constant; it may change frequently and be shared between several devices. The originating IP address of a communication is routinely gathered in many types of internet transaction, but if the CSP does not hold information on which of its subscribers held which IP address at a particular point in time it is very hard for law enforcement authorities to prove an association between an action on the internet and a particular individual. Not all United Kingdom providers currently obtain all the data necessary to trace which subscriber is using which IP address. During the course of our inquiry we heard of various circumstances in which the lack of this data has impeded investigations. We accept that if CSPs could be required to generate and retain information that would allow IP addresses to be matched to subscribers this would be of significant value to law enforcement. We do not think that IP address resolution raises particular privacy concerns.

75. **We recommend that a narrower clause 1 should allow notices to be served on CSPs requiring them to generate and retain subscriber data relating to IP addresses.**

76. The term "web logs" is used to refer to a record of information that relates to a communication between a user and the internet. This would include connections to the world wide web (i.e. what websites a person has accessed) and also contacts with other internet services, such as smart phone applications.

77. The Code of Practice for the Acquisition and Disclosure of Communications Data makes clear that this type of data can be accessed by law enforcement agencies if it is held by CSPs. It provides that anything before the first "/" in a website address is considered to be communications data, and anything after the first slash is considered to be content. So the fact that a person visited www.nhs.uk is communications data and could form part of a web log, but it would not be permissible to record the fact that a person visited www.nhs.uk/conditions/depression. Under the current law if a CSP keeps web log data for business purposes then an order can require them to retain that data for 12 months, but if

web logs are never generated—and most CSPs do not generate them for business purposes—there can be no requirement to make them available.

78. Sir Peter Fahy, Chief Constable of Greater Manchester Police, told us that if it were possible to reconcile IP address and subscriber information and also to identify which websites were visited by a service user this would resolve the data gap,[62] and Peter Davies, Chief Executive of CEOP, agreed,[63] but neither of them provided examples that proved the importance of web logs or referred to cases that had been hampered by the current lack of web log data. The one piece of evidence we saw that went some way to proving a need was during our visit to the Metropolitan Police Service,[64] when officers used real life cases to illustrate how it is hard to identify whom a suspect is communicating with if those communications are conducted over the internet on a mobile phone. Those cases showed that it would be useful to know if suspects were using a website that allowed them to communicate with others because the CSP running that website could then be asked for information about who was contacted. To do this it would be necessary to know the website visited and the IP address assigned to the suspect at that time (so the website could be asked to check who the user of that IP address contacted). This illustrates the Home Office's case that the need for IP address information and the need for web log data are connected.

79. The kinds of investigations where it is possible to imagine web logs being useful include: enabling the identification of internet services used by a suspect so that further communications data requests can be made from those services; investigating the web log associated with a sex offender to determine whether they had accessed known child abuse websites; and investigating whether a suspect had accessed a known terrorist website.

80. We have received considerable evidence expressing concern at the idea of web log data being more widely retained and made available to public authorities. A submission signed jointly by representatives from Liberty, Justice, Privacy International, the Open Rights Group, Big Brother Watch and NO2ID made the case that web log data should not fall under the definition of communications data, even though it does already, because it has the potential to reveal considerable personal information about an individual:

> "Throughout her oral evidence the Home Secretary sought to articulate a distinction between the content of a communication and the communications data which she characterised as the "who, when, where, how" of a communication.... A record of the addresses of websites visited patently reveals a great deal that is substantive and potentially extremely personal about an individual's life. An individual's browsing history is liable to betray his or her political inclinations, state of health, sexuality, religious sentiments and a huge range of other personal characteristics, preoccupations and individual interests besides. We fail to see that the distinction drawn by the Home Secretary can have any meaning at all if communications data is deemed to include information of this nature."

62 Q 1096

63 Ibid.

64 See Appendix 4.

81. Retaining web log data would place massive storage demands on CSPs and this would be costly. Some witnesses also expressed concerns that the more information that is stored, and the more sensitive the nature of that data, the greater the chance of a security breach. Given the potentially sensitive nature of web logs, a security breach could be particularly damaging for the individuals whose data was lost. The secure storage of communications data is addressed in Chapter 5. Briefly, it is possible (given a willingness to accept the necessary cost) to achieve a high degree of security of storage. But no one has claimed or could claim that total 100 per cent security can be guaranteed: there is bound always to remain the possibility of a breach, whether as a result of skilled hacking or because of human error or misfeasance.

82. We accept that web logs are a type of communications data from which significant inferences could be drawn about a person's interests and, perhaps, activities. Web logs are at the more intrusive end of the communications data spectrum and it is at that end that the need for rigorous safeguards is most acute. Safeguards are discussed in Chapter 5. We believe that the SPoC and Designated Senior Officer system now in force, if operated by properly trained and experienced staff, and subject to the safeguards proposed in the draft Bill and the strengthening of those safeguards we are recommending, can provide sufficient safeguards against abuse within the system. The fact that web logs would be accessible only by certain pubic authorities, that access would be on a case-by-case basis and only when access was necessary and proportionate, and the fact that access would be subject to independent review, are also important.

83. One way of reassuring civil liberties groups and more importantly the general public, while at the same time satisfying the needs of law enforcement agencies, would be to devise a definition of web service that covered only those that could be used as a method of communication. This would cover websites offering e-mail and other messaging services, but not websites that simply supply information. CSPs could then be required only to keep web logs in so far as they related to visits to communications sites. This would however prevent, for example, a CSP from being required to keep records of visits to a site thought to be accessed by terrorists unless that site also enabled users to communicate with each other, or to post messages. Whether or not this would be technically and operationally feasible, and if it was what the associated costs would be, is not something that we have had time to explore.

84. **Whether clause 1 should allow notices that require CSPs to retain web logs up to the first "/" is a key issue. The Bill should be so drafted as to enable Parliament to address and determine this fundamental question which is at the heart of this legislation.**

85. **The Home Office and law enforcement agencies and (so far as we know) the intelligence and security services think that access to weblogs is essential for a wide range of investigations. The civil liberties organisations argue that web logs are potentially a highly intrusive form of communications data and that generating and storing web logs gives rise to unacceptable risks to the privacy of individuals.**

86. **We are confident that the safeguards in the draft Bill, together with the recommendations we make to strengthen those safeguards, can provide a high degree of protection against abuse of communications data or inadvertent error by public authorities. We acknowledge that storing web log data, however securely, carries the**

possible risk that it may be hacked into or may fall accidentally into the wrong hands, and that, if this were to happen, potentially damaging inferences about people's interests or activities could be drawn. Parliament will have to decide where the balance between these opposing considerations should be struck.

87. **In 2003, Parliament considered the Code of Practice for the Acquisition and Disclosure of Communications Data which included the guidance that web addresses up to the first "/" should be considered to be communications data. The presentation of this Bill provides an opportunity for Parliament to review this controversial issue.**

88. **We also recommend that the Home Office should examine whether it would be technically and operationally feasible, and cost effective, to require CSPs to keep web logs only on certain types of web services where those services enable communications between individuals.**

Third party data

89. The Bill is intended to require CSPs operating in the United Kingdom, whether based here or abroad, to comply with retention orders served under clause 1 and disclosure requests made by public authorities. As will be made clear in Chapter 6 there are likely to be significant problems with getting CSPs based overseas to recognise the extra-territorial application of United Kingdom legislation, and there will inevitably be cases where overseas CSPs both refuse to retain the data that the United Kingdom Government asks them to retain and refuse to disclose the data that public authorities need. It is not clear, given the level of informal assistance currently offered by the largest overseas based CSPs to disclose information to investigators, especially in urgent cases where lives are at immediate risk, how significant a problem this actually is. Some overseas based CSPs are likely to take a more pragmatic approach than others. It is because of the variable approaches of the different overseas CSPs to providing communications data that the Home Office argues that power is also needed under clause 1(3)(c)(ii) to require United Kingdom CSPs to store and disclose communications data traversing their networks which relates to services from other providers. This is commonly referred to as the third party provision. A simple illustration is that using the third party provision it would be possible to ask a United Kingdom broadband provider to collect data on e-mails crossing its network when those e-mails were sent using one overseas based e-mail provider to another overseas based e-mail provider.

90. The third party provision has proved particularly controversial both because of technical concerns and because, as LINX put it, "The collection and processing of "third party" communications data by network operators is a substantial extension of their duties that is, in our opinion, materially distinct from existing data retention requirements, amounting to a complete novelty". Big Brother Watch agreed, saying that if these provisions are passed UK CSPs could in future be described as "private surveillance operations".

91. To understand the technical concerns it is useful to understand a little about how third party data would be collected. It would be necessary to place data probes within a CSP's network and those probes would be programmed to generate information from network links within the CSP. Deep Packet Inspection (DPI) would be used to isolate key pieces of

information from data packets in a CSP's network traffic. The Home Office seemed confident that this was technically possible. Other witnesses questioned whether it is technically feasible to extract meaningful and helpful information from third party services. One of the primary technical challenges would be dealing with encrypted data.

92. Many internet services are encrypted; this includes many of the major overseas based communications services such as Gmail. Encryption is the basis of internet security and companies encrypt their services to protect their customers. If these companies are asked directly for communications data and agree to supply it, whether under RIPA or following a request under a Mutual Legal Assistance Treaty (MLAT), then they will decrypt the information, extract the relevant communications data and provide it to the requesting authority in an accessible format. They told us however that if information about their service was collected by another CSP they would not cooperate in helping decrypt it. Sarah Hunter from Google explained:

> "From a Google Inc perspective, we are very confident about the security of our encryption. If a valid RIPA request comes in or UK law enforcement goes through the MLAT, receives a court order and in turn gets Gmail user data, we will obviously provide that data decrypted. If it was to use a third-party provider to gather the encrypted data, I think it very unlikely that Google Inc would provide anyone outside Google Inc with that key. That is simply because, as everyone said earlier, security is our most important asset. Our relationship with our users is predicated on trust. Without that, we have no business".[65]

93. Several witnesses questioned whether valuable communications data could be retrieved from encrypted services. Services encrypt not only content but much of the communications data too, and the UK CSP whose network the encrypted service is crossing will not be able to decrypt the package, nor could they legally do so because to do so would be to intercept content. As Everything Everywhere put it, "even if we were able to decrypt, you would have to open the whole packet, and then you are looking at the content".[66] UK CSPs will not be able to hand over the whole encrypted package to law enforcement or the Home Office because to do so would be to hand over content.

94. Bob Hughes, Government Programme Manager at Telefónica UK–O2, gave a helpful illustration of the kind of data that a UK CSP would be able to provide about an encrypted third party service:

> "When we are talking about picking up third-party data, we are now talking about gateway-to-gateway data. This is very similar to a lot of letters having been passed to a delivery box on one side of the network, put into a big courier delivery box and crossing our network to a terminating distribution box on the other side. Then, all those letters are taken out of the box and sent on to their various places... All that we will see when we look at those encrypted data are the two points of the gateway. We are storing all of these communications, which are just gateway-to-gateway. We cannot hand over the whole box because we know that that includes content. We can give you only the piece that is on the outside of the box that includes all the

65 Q 595

66 Q 438

> encrypted data. Therefore, the value, by comparison with the letter and its journey from A to B, is much reduced."[67]

95. Although this may sound of limited utility Home Office officials said it could still be valuable to ongoing investigations: "Encrypted data can still be very important and can give you unencrypted chunks of data which are relevant to the three questions which we are asking ourselves and to which we come back all the time."[68]

96. One of the significant risks of the third party provision is that it may actually lead to an increase in the number of services that use encryption, and this could actually reduce the amount of communications data available to in the United Kingdom, a serious unintended consequence directly at odds with the stated purpose of the legislation. Evidence that this was a real risk came from Simon Milner, the Director of Policy for UK and Ireland of Facebook, who explained:

> "The security of our networks and the security of how we store and look after customer data are fundamental to our businesses. Therefore, when we are concerned that someone else might be trying to intercept our data, we will move heaven and earth to ensure the security of our network. It is a grave concern to us that it might well be part of the new framework that UK CSPs might be required to retain these data. One would expect there to be not only implications for relationships in the internet value chain but changes in behaviour by users. Facebook users already have the ability to encrypt their traffic, and we would expect many more UK users to choose to do so were that kind of measure to be introduced".[69]

97. This issue was also highlighted in evidence from Virgin, ISPA and Telefónica UK–O2.[70]

98. Microsoft questioned how a United Kingdom CSP would identify which encrypted information it would be necessary to store in order to comply with a third party provision notice:

> "How can we guarantee that the CSP has identified the right packets to be stored? Multiple providers, Skype included, use obfuscation techniques precisely to avoid being detected by deep packet inspection equipment. My question is a technical one: how would they guarantee that they would be storing the correct data under the order?"[71]

99. There are some instances of services that not only encrypt but have specific software to ensure no communications data is kept about their users, and no websites can identify their users when they visit. For example, we took evidence from the Tor Project, a not-for-profit organisation which encrypts and redirects its users' communications to ensure they cannot be traced. The Tor Project is used by people trying to circumvent national censorship schemes, by victims of crime, by military personnel working undercover, by journalists wishing to protect their sources and by whistleblowers.

67 Q 435

68 Charles Farr, Q 933

69 Q 628

70 Q 26

71 Stephen Collins, Q 632

100. Encryption is not the only technical challenge posed by the third party provision. We received evidence questioning whether DPI technology could cope with the level of traffic that moves across service provider networks. ISPA stated that "DPI and such technology can be used by ISPs for legitimate traffic management processes, but it does not follow it could be repurposed to fulfil the requirements set out in the draft Bill. We are yet to be convinced that current hardware can handle the volume of traffic that moves across service provider networks at this level".

101. One of the key technical challenges would be to programme DPI systems to isolate communications data information from the content of messages sent. Even BAE Systems Detica, who as manufacturers of DPI technology were confident of its capabilities, admitted that it would be challenging to keep the DPI systems up to date with changes that originating CSPs make to the underlying formats and protocols used by those services.[72] The pace at which CSPs change their systems (particularly proprietary ones) can be very fast. This means that DPI system manufacturers and CSPs would need to devote significant resources to monitoring and updating systems both to maintain coverage and to operate correctly. Microsoft confirmed this:

> "We have a dedicated team involved in this obfuscation constantly in order to protect the integrity of the communications. At the same time, DPI equipment manufacturers have guys on the other side trying to work out what we are doing. That will continue. The point about it from the perspective of this draft Bill is that it costs money to maintain DPI equipment. We do not just buy once; there is a constant need to pay to have it updated in order for it to perform. That is the key here—it is very expensive".[73]

102. The concerns about the third party provisions are not limited to questions about their technical feasibility. UK CSPs would find it challenging to understand even non-encrypted communications data belonging to other services. Under the current system the Home Office works with CSPs to categorise their data, agree what should be exempted as content, and then list the data available in the "SPoC book". Only the company that generates the data can give an informed opinion about how the data should be categorised. A third party will not easily be able to judge whether a law enforcement agency is right to categorise a request for third party data as, for example, "subscriber data", or even as data rather than content. The only data type the third party could confidently identify is traffic data. This was illustrated by Jonathan Grayling from Everything Everywhere: "I think we could probably stand a pretty good chance of identifying what is content and communications data in our own data, because we understand it: we understand how our systems work and how we interpret it. But to understand third-party data, even if it is not encrypted, is going to provide challenges".[74]

103. The UK CSPs were also concerned about the commercial implications of the third party provision. They rely on good relationships with the main internet service providers, many of whom are based overseas. If some of those providers choose not to cooperate with this legislation but are aware that UK CSPs may be ordered to collect data on their services,

72 Evidence given in private; this reply cleared for publication.

73 Stephen Collins, Q 634

74 Q 500

then this could change the nature of their relationship. This was a significant concern for the UK CSPs.[75]

104. The cost of constantly reprogramming DPI probes to keep abreast of changes to third party services has already been mentioned. This is not the only significant cost concern. The cost of the DPI probes themselves would be significant, and that and the costs of the large scale storage demands worry the UK CSPs.[76] Their concerns will be explored further in Chapter 7.

105. Given the significant concerns about the third party provision some witnesses have called for it to be dropped.

106. When the UK CSPs gave evidence to us in September they stated that Home Office officials had given them oral assurances that the third party provision would be invoked only after the original service provider had been approached and all avenues to get them to comply with requests for communications data had been exhausted. The UK CSPs also said they had been given assurances that they would not have to decrypt third party data. These reassurances were important to them and they were very concerned that there was nothing in the Bill to back-up the Home Office's promises.[77]

107. We explored this issue with Home Office officials in October and Charles Farr repeated the reassurance he had given the UK CSPS:

> "I think they [the UK CSPs] were under the misapprehension that we might go to them to collect third-party data, even before asking the third-party to cooperate with us. They were understandably concerned if that were to be the case. Were it to be the case, the costs would be rather different from what they otherwise might be. I hope we have reassured them. I would repeat, if I may, that it would be in extremis for us to go to them and ask for the collection of third-party data. In the vast majority of cases we do not expect to, and we have calculated the costs accordingly."[78]

> "If they cannot distinguish communications data from content they will not be required to retain it. We are not asking for the storage of masses of encrypted data."[79]

108. When asked whether he agreed that the legislation should reflect these assurances Charles Farr agreed to look at it.[80] We note that the Intelligence and Security Committee has recommended that "the Home Office should have to demonstrate due diligence before resorting to the use of DPI to collect communications data from overseas CSPs" and that this should be reflected on the face of the Bill.

109. **The Home Office knows that not all overseas CSPs will comply with retention notices. It is for this reason that the notices issued under the order-making powers in clause 1 may require UK CSPs to keep third party data traversing their networks. UK**

75 e.g. Virgin Q 420, LINX written

76 e.g. see Vodafone and BT Q 452

77 e.g. Everything Everywhere, Q 422

78 Q 883

79 Q 933

80 Ibid.

CSPs are rightly very nervous about these provisions. The Home Office has given an oral commitment to UK CSPs that the Home Secretary will invoke the third party provisions only after the original data holder has been approached and all other avenues have been exhausted. The Home Office has also given a commitment that no CSP will be asked to store or decrypt encrypted third party data. These commitments should be given statutory force.

Filtered data

110. Clause 14 provides a power to establish filtering arrangements to facilitate the acquisition of communications data. The Request Filter would be used for complex communications data inquiries that cover several CSPs. As the Home Office explained, "Internet communications services are technically different from the telephone services of the past. The communications data now needed to understand the 'who, how, when and where' of a single communication may no longer be held by a single communications provider".[81] Rather than a public authority having to submit separate requests to several CSPs, it would submit one request through the Request Filter which would then interrogate the multiple CSP databases and automatically analyse the returns, providing investigators with only the relevant data. CSPs could design their systems to allow full automation of requests through the filter, or they could decide to have staff check each request before allowing the Request Filter to access data. It is important that CSPs have this choice.

111. The Government's case for the Request Filter is that it "is intended to enable law enforcement agencies to continue acquiring complex communications data in a way that minimises collateral intrusion".[82] The Home Office sees the benefits as: minimising human error, speeding up complex requests and minimising collateral intrusion. The Request Filter is little different from the work that investigators currently carry out comparing data from multiple CSPs when dealing with complex enquiries. The difference is that it will be an automated process which may be faster and less prone to human error, but will require significant work to develop and will require the Home Office to impose technical requirements on each provider to ensure that data from the provider's systems is always returned to the Filter in the same technical format, thus facilitating easy data comparison.

112. The Home Office is at pains to assert that the Request Filter is not a central database: "The legislation makes clear that the Filter can only acquire and process communications data to answer a specific public authority request. Once that request has been answered the Filter will permanently delete all the communications data it acquired".[83] The Home Office emphasise this point because in May 2008, when the last Government announced plans for legislation which would have required communications data to be stored for a year in a purpose-built database, the plans were heavily criticised, not least by the two Parties that now make up the coalition Government.

113. It is however important to consider how different the proposals for the Request Filter really are from the previous Government's proposals for a central database. A central

81 Written evidence, paragraph 113

82 Ibid.

83 Written evidence, paragraph 118

database would have been one repository of communications data provided by the CSPs but stored on a Government owned and operated database. The Request Filter is a Government owned and operated data mining device which, to work efficiently, requires each CSP to maintain its own database of all its communications data in a common format. Each CSP database will be able to be accessed at any time by the Request Filter. So the same data is being stored about the same people and it is being stored in databases which are accessible to public authorities given powers under the Bill. The difference is that instead of one database there are many and they are privately owned. Although they are privately owned the Government can stipulate what should be held on them, for how long, and in what format it should be supplied. The differences therefore are not as great as the Home Office suggests; the Request Filter can be equated to a federated database.

114. There is also vigorous debate about whether the Home Office is right to argue that the Request Filter minimises collateral intrusion and thus is a tool in protecting privacy. On the contrary, many witnesses see it as a threat to privacy. For example LINX stated that:

> "Clauses 14-16 establish a requirement that communications data be processed and assembled by matching related data from different operators, such that the relationships between diverse data elements relating to a particular user are capable of being machine-processed as such. In other words, the draft Bill requires the functional equivalent of building communications data profiles on every user, which will contain everything within the definition of communications data, including time and geolocation data".

115. LINX point out that it would be technically possible to "perform profile searches of the following format: 'List all persons who are the designated user of a mobile phone that was in Location (e.g. Trafalgar Square) at Time (e.g. noon last Tuesday), and who have read any of the following websites more than once in the past period (e.g year)' ".

116. There are also questions as to whether the Filter amounts to a "general monitoring" obligation, contrary to Article 15 of the EU E-Commerce Directive.[84] This is not something we have had time to investigate but it is an issue the Home Office should consider.

117. The Request Filter would make it technically possible to perform profile searches on individuals. If it was used in this way there is a risk that it could amount to general monitoring, but there are safeguards to prevent this. Every request to the Request Filter will have to go through the same authorisation process set out in Chapter 2. This includes a requirement to explain why the request is necessary and proportionate, and needs the authorisation of a Designated Senior Officer. In addition the draft Bill puts obligations on the IoCC to monitor the operation of the Request Filter and examine the audit trails produced. This safeguard is key, as Professor Peter Sommer told us:

> "If these safeguards are not rigorously applied and fully examined by the Interception of Communications Commissioner there is a risk that that what is

84 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 (OJ L178 of 17 July 2000). Article 15(1) provides: "Member States shall not impose a general obligation on providers … to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity."

> described as "request filtering" becomes large-scale data mining; the necessity and proportionality tests need to be applied not to just the individual data streams as supplied by CSPs but to the likely effect when they are assembled together."

118. We consider in the following chapter the role of the IoCC in maintaining public confidence in the Filter.

Who will design, programme and maintain the Request Filter?

119. The draft Bill makes the Secretary of State responsible for setting up and maintaining any filtering arrangements, and provides the power to transfer this responsibility to a designated public authority. Day to day operation of the filtering arrangements may be carried out by an approved body. Evidence from the Home Office suggests that if the Secretary of State was to transfer her powers to a designated public authority it would be to the new National Crime Agency.[85] The scope of the Bill does not limit who the day to day operation can be transferred to, and some witnesses have expressed concern that it could be GCHQ which is not accountable to the public or to Parliament, although any transfer of functions would not affect the Secretary of State's responsibility for the exercise of the functions.

120. Some witnesses have questioned whether it is appropriate that the Secretary of State should be responsible for the operation of the Filter. Professor Peter Sommer argued that "making this a function, direct or delegated, of the same Secretary of State who also issues interception warrants and orders under the draft Bill is surely a mistake; if there is to be a credible and viable independent filtering agency much more needs to be said about its resources and governance."

121. The Request Filter will be a very complicated piece of technology. It will need to be constantly updated as new CSPs are added, existing CSPs merge or CSPs change the kind of communications data they have available and the format in which it is held. Witnesses have expressed concern that the public sector will not be able to attract and retain programmers of sufficient skill to design and maintain a robust and effective filter. Professor Peter Sommer wrote: "it will need resources, among them highly skilled staff who are familiar with the law, the applicable technologies and police investigative procedure – and who can also act independently. They will almost certainly need high levels of security clearance. In the private sector such people are likely to earn fairly high income; moreover they will want some form of career structure and stability. But there may not be a sufficiently consistent flow of work to make this possible."

122. **Whoever operates the Request Filter will need significant expertise and staff at their disposal. If CSPs update their system and the Request Filter is not adjusted there is a risk that results will be incomplete, rendering them useless. The Bill should be amended to say that the Secretary of State may transfer her responsibilities for operating the Request Filter to the soon to be established National Crime Agency but not to other bodies. The National Crime Agency will need appropriate resources and this should be reflected in the revised cost/benefit analysis.**

85 Q 94

Evidential quality of Request Filter results

123. The Home Office's written evidence explains that "It will be possible to manually check that the Filter had functioned correctly (to ensure that the result is sound) that there will be an audit trail of filter requests."[86] We were not provided with information about how detailed this audit trail will be and how the audit trail sits with the requirements that "once the processing and filtering to answer a request is complete all acquired communications data is immediately destroyed". The quality of the audit trail is important because if Request Filter results are to be used as evidence in criminal proceedings, whether for the prosecution or the defence, they will need to meet evidential standards. Several of our witnesses, including LINX, questioned whether they would.

124. However the Director of Public Prosecutions was not concerned that results from the Request Filter might not meet evidential standards. His view was that although there would be challenges the Filter arrangements were "workable provisions".[87] This was also the view of Lord Carlile of Berriew QC[88] and the IoCC.[89]

125. It is our view that the quality of the audit trail will be key to ensuring that results from the Request Filter meet evidential standards. It will be necessary for the prosecution to prove that a result from the Filter is robust and reliable. To do this they will need a clear audit trail that enables them to re-run the data processing exercise in order to satisfy the jury that the correct questions were asked of the Filter and that the results were accurate. This will require data needed for criminal proceedings to be held for more than 12 months; this includes the collateral data that the Filter will have excluded from the result it provided. Without that collateral data a request could not be recreated.

126. **The Request Filter will speed up complex inquiries and will minimise collateral intrusion. These are important benefits. On the other hand the filter introduces new risks, most obviously the temptation to go on "fishing expeditions". New safeguards should be introduced to minimise these risks. In particular the IoCC should be asked to investigate and report on possible fishing expeditions and to test rigorously the necessity and proportionality of Filter requests.**

Accessible by whom?

127. We explained in Chapter 2 that, of the many public authorities currently allowed to access communications data, the only ones listed in section 25 of RIPA are police forces, SOCA (soon to be replaced by the new National Crime Agency) and the Scottish Crime and Drugs Enforcement Agency (SCDEA), HMRC and the intelligence and security services. "Police force" and "intelligence service" are defined in section 81(1) of RIPA. All other public authorities permitted to access communications data are empowered to do so by order of the Secretary of State. Clause 21(1) of the draft Bill follows exactly the same pattern, save that the SCDEA do not appear in the list. Again, if any other public

86 Paragraph 117

87 Q 819

88 Supplementary written evidence

89 Q 689

authorities are to be added to the list, this would be by order of the Secretary of State, subject to affirmative resolution.

128. We are satisfied that the four main users currently listed in the draft Bill—the police, SOCA, HMRC and the intelligence and security services—should remain on the face of the Bill as public authorities allowed access to communications data. Together they currently account for 99% of requests for communications data, and we have no doubt that they should continue to have access to it, subject always to the enhanced safeguards we suggest in Chapter 5.

129. We have considered whether there are other authorities for which an equally strong case can be made, so that they too should be listed in the Bill even though the use they make of communications data is on a smaller scale. We believe that there are two such bodies. The first is the Financial Services Authority (FSA). In the last three years it has made 5,459 requests for access to communications data,[90] 2,325 of them in 2011.[91] The matters it deals with are of increasing importance. The second is the UK Border Agency (UKBA). It is not listed as such in the current Order:[92] instead there is a reference to the Home Office, but the persons designated to grant authorisations are officials of the UKBA. They have made 10,103 requests in the last three years,[93] some dealing with key immigration offences such as people smuggling and trafficking, in addition to more routine immigration crimes. The UKBA too should in our view appear on the face of the Bill, but under its own name rather than as the Home Office.

Local authorities

130. Of some 600 public authorities authorised to access communications data, over 400 are local authorities, which are permitted to acquire subscriber data or use data but not traffic data. Trading standards departments are the principal users of communications data within local authorities, although the environmental health departments and housing benefit fraud investigators also occasionally make use of the powers. Local authorities enforce numerous statutes and use communications data to identify criminals who persistently cheat consumers, the taxpayer, deal in counterfeit goods, and prey on the elderly and vulnerable. The environmental health departments principally use communications data to identify fly-tippers. [94]

131. In 2011 141 local authorities notified the IoCC that they had made a total of 2,130 requests, which is just 0.4% of all communications data requests submitted by public authorities. Despite this, local authorities accounted for 9% of the reportable errors. The evidence we received shows that errors by local authorities cause public concern out of all proportion to the numbers involved. This seems to be because examples of misuse or abuse of the system are not only relatively frequent, but also particularly alarming.

90 Home Office Business Cases for Public Authorities not currently listed in the draft Communications Data Bill.

91 2011 Annual Report of the Interception of Communications Commissioner, HC 496.

92 The Regulation of Investigatory Powers (Communications Data) Order 2010, SI 2010/480.

93 Home Office Business Cases for Public Authorities not currently listed in the draft Communications Data Bill.

94 2011 Annual Report of the Interception of Communications Commissioner, HC 496.

BOX 6: Failure of authorisation by local authorities

The IoCC found that in 2011 two local authorities made a total of 52 requests which were not approved by a person of sufficient seniority to act as a designated person, and were therefore unlawful. In one of those authorities the same person had acted as the applicant, SPoC and designated person, so that there was a complete lack of scrutiny; in effect the requests were self-authorised. In two instances in two different local authorities the SPoCs processed and the designated persons approved the acquisition of traffic data, which local authorities are not permitted to acquire.

132. The IoCC reported one case where a local authority used communications data in relation to a matter which was not a criminal offence at all, and did not come close to being a permitted purpose.

BOX 7: Use of communications data for an unauthorised purpose

An allegation was made that a parent living outside the catchment area of a school provided an address within the catchment area to secure a school place. Communications data was requested to provide evidence of residence and to confirm the genuine address. The application stated that the Schools Admissions Department would withdraw the place for the child if the allegation was substantiated, but no criminal offences were specified. Nevertheless the application was authorised and the data released.

133. This was a case which caused considerable public disquiet; no fewer than seven of our witnesses referred to it in written evidence. [95] What causes us still further disquiet is the statement from the IoCC that "I was satisfied from this that the conduct undertaken by the Council did not amount to wilful or reckless use of the powers. It is clear that the Council went through a considered thought process, that legal advice was sought prior to submitting the application and that there were ongoing discussions in relation to whether a prosecution was feasible." This does nothing to allay our own anxieties. It scarcely needs legal advice to work out that the support of a schools admissions policy is not a proper use of communications data. Sir Paul Kennedy has also argued that "The controls are perfectly in place. I know there has been the odd incident about the school catchment area, or something like that, but they are the odd incident and if there is a criticism—and I have said this in a report before—it is that local authorities do not always use these powers as much as perhaps they ought to, to deal with the type of offending that they are entitled and required to investigate, and probably have no other means of investigating."[96]

134. The IoCC reports that, of the 141 local authorities which notified him that they had made use of their powers in 2011, 58% had made fewer than 10 requests. This plainly contributes to the number and gravity of the errors: those processing applications for access to communications data do so infrequently and have relatively little experience of the system. When local authorities were added to the list of relevant public authorities[97]

95 This has to be distinguished from a similar case of a local authority using directed surveillance powers under Part II of RIPA, and not powers under Chapter II of Part I (*Jenny Paton and others v Poole Borough Council* (2010) IPT/09/01/C) http://adam1cor.files.wordpress.com/2010/08/investigatory_powers_tribunal_ruling.pdf

96 Q 678

97 by Article 3 of the Regulation of Investigatory Powers (Communications Data) Order 2003, SI 2003/3172.

there was no suggestion that applications by them should be subject to a different procedure from applications by other public authorities. However the Coalition Agreement included the following undertaking: "We will ban the use of powers in the Regulation of Investigatory Powers Act (RIPA) by councils, unless they are signed off by a magistrate and required for stopping serious crime."[98] Section 37 of the Protection of Freedoms Act 2012, which came into force on 1 November, added to RIPA two new sections 23A and 23B, the effect of which is that authorisations for local authorities to access communications data do not take effect unless and until approved by a justice of the peace in England and Wales, a sheriff in Scotland, or a district judge (magistrates' courts) in Northern Ireland.

135. There are thus historical reasons why, in the case of RIPA, it is the Act which provides the conditions subject to which local authorities can access data, even though it is not the Act itself which grants them the right of access. We can see no reason why the draft Bill should follow this pattern; yet clause 11 specifies that judicial approval is needed for access by local authorities, which are defined by clause 21(1), even though they would have no right at all to access communications data unless under the Bill, once enacted, the Secretary of State made an order permitting such access.

136. If it is thought that local authorities, or some of them, should have access to communications data, they should follow the procedure we have suggested for all other public authorities. We deal in the following chapter with the question of the conditions which should apply to any access by local authorities.

137. **Any public authorities which make a convincing business case for having access to communications data should, like the six we have specified in paragraphs 128 and 129, be listed on the face of the Bill. We expect this to be a greatly reduced number when compared to the authorities currently listed in the Regulation of Investigatory Powers (Communications Data) Order 2010.**

138. **Any necessary changes to this list should be made by order subject to the super-affirmative procedure which includes the opportunity of scrutiny by the appropriate Select Committee.**

Accessible for what purposes?

139. Clause 9(6) of the draft Bill sets out the purposes for which it is permissible to access communications data. It reads:

> (6) For the purposes of this section it is necessary to obtain communications data for a permitted purpose if it is necessary to do so—
> (a) in the interests of national security,
> (b) for the purpose of preventing or detecting crime or of preventing disorder,
> (c) for the purpose of preventing or detecting any conduct in respect of which a penalty may be imposed under section 123 or 129 of the Financial Services and Markets Act 2000 (civil penalties for market abuse),
> (d) in the interests of the economic well-being of the United Kingdom,

98 Chapter 4: Communities and Local Government.

(e) in the interests of public safety,
(f) for the purpose of protecting public health,
(g) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department,
(h) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health,
(i) to assist investigations into alleged miscarriages of justice, or
(j) where a person ("P") has died or is unable to identify themselves because of a physical or mental condition—
  (i) to assist in identifying P, or
  (ii) to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition.

140. Purposes (a), (b) and (d) to (h) were in RIPA as originally enacted. Purposes (i) and (j) were added in 2006 by Order[99]—the only such additions. Only purpose (c) is new. Schedule 2 to the draft Bill would amend section 175 of the Financial Services and Markets Act 2000 so that the FSA could not require CSPs to disclose data for the purposes of investigations. Conversely, under paragraph (c) data could be obtained to prevent or detect conduct which would not necessarily constitute a criminal offence. We are satisfied that this is a legitimate purpose, and it is for this reason that we stated in paragraph 129 that a good case can be made for adding the FSA to the list of public authorities on the face of the Bill.

141. Much the most common reason for requesting and accessing communications data is "preventing or detecting crime"—purpose (b). "Crime" can of course include trivial offences, and only the requirements of necessity and proportionality can prevent communications data being used for such crimes. But in evidence to us the Home Secretary was referred to an article she had written in The Sun, where she had said that "Only suspected terrorists, paedophiles or serious criminals will be investigated under the Bill". She confirmed that this was the "main purpose" of the Bill.[100]

142. The draft Bill has annexed to it the Home Office memorandum on compatibility with the ECHR, and in particular with Article 8, the right to privacy. Article 8 reads:

> "(1) Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> (2)There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

99 The Regulation of Investigatory Powers (Communications Data) (Additional Functions and Amendment) Order 2006, SI 2006/1878 which is now consolidated by the Regulation of Investigatory Powers (Communications Data) Order 2010, SI 2010/480.

100 QQ 1158-1159

143. Article 8(2) is tantamount to an exhaustive list of permitted purposes; no purpose which does not fall within those words would be permissible. Two such purposes have been added in the space of 12 years. It is now proposed to add a third. We believe it is unlikely that a good case can be made for yet further permitted purposes. Clause 9(7), like the existing provision in RIPA, would allow the Secretary of State, by order subject to affirmative resolution, to add yet more permitted purposes. However the Home Secretary told us: "We have certainly got no intention of setting out any permitted purposes beyond those that are in the draft Bill."[101]

144. We sought the views of the House of Lords Delegated Powers and Regulatory Reform Committee on clause 9(7), and their conclusion was that "were a Bill to be introduced containing the same power as in the draft, we would not necessarily find it acceptable just because it derives from existing legislation." We agree. We believe that any additions of further permitted purposes should be by primary legislation, and that clause 9(7) should be deleted.

145. The fact that there are ten permitted purposes does not mean that relevant public authorities should have access to communications data for all those purposes. Currently no authority, not even any of the four core authorities, is permitted access for all these purposes. The police do not need, and do not have, permission to access data for tax purposes or to investigate miscarriages of justice. Only HMRC need, and have, access for tax purposes; only the Criminal Cases Review Commission, and its Scottish equivalent, need and have access to investigate miscarriages of justice, and they have access for no other purpose. The fire and ambulance services routinely have access only in the case of life-threatening emergencies. These are important limitations. Scrutiny of draft orders which would add public authorities to the list of those permitted access to communications data should ensure that access is permitted only for those purposes which are strictly necessary.

146. **Of the ten permitted purposes in clause 9(6) of the draft Bill, seven were in RIPA originally, two were added by order in 2006, and one is new. We think it unlikely that there are any other as yet unidentified purposes which could properly be added. The House of Lords Delegated Powers and Regulatory Reform Committee has recommended that any additions to this list should require primary legislation. We agree. Clause 9(7), which allows the Secretary of State to add further permitted purposes by order, should be deleted.**

147. **We are concerned that the long list of permitted purposes for which communications data can be requested adds to public disquiet about the breadth of the Bill. While we do not make specific recommendations about how this list could be shortened, we recommend that the Government should consult on whether all the permitted purposes are really necessary.**

101 Q 1158

5 Safeguards

148. The draft legislation includes various safeguards to ensure that the communications data regime operates safely and effectively with checks and balances. Some of these safeguards are not as strong or as clear as they could be.

Definitions of communications data

149. We believe that one of the central safeguards is ensuring that the definitions in the draft Bill are clear and appropriate and do not raise the risk that communications data will include information other than what is really needed by law enforcement and other bodies.

The definition of content

150. The Government has repeatedly assured us that nothing in the draft Bill will allow access to the content of a communication. The Home Secretary emphasised this point: "I am absolutely clear that the key data we want is the who, when, where and how. That is clear, and there is no intention of going beyond that into content or anything..."[102] There is nevertheless debate about whether the legislation ensures that content cannot be accessed.

151. Clauses 1(4) and 9(5)(a) both explicitly prohibit the interception of communications in the course of their transmission. Content itself is never defined in the legislation, although it is referred to. The draft Bill's definition of "use data" explicitly excludes the content of a communication but the definitions of traffic and subscriber data have no similar exclusions (see Box 8).

152. These drafting issues have given some of our witnesses the impression that traffic and subscriber data may include content. For example, JANET, a private data network that connects universities, colleges, research organisations and schools networks to each other and to the internet, stated in its written evidence that "Indeed since, unlike clause 28(4) defining use data, clause 28(5) does not exclude the content of communications, it appears that communications data would also include the content of all the user's messages that were held by the telecommunications operator".

153. This illustrates a common fear. The content of user messages (e-mails, stored voicemails, texts, closed Facebook posts, closed blog postings etc) would not be covered by this legislation. If the drafting gives the impression that these things could be accessed then the definitions should be revisited to give public reassurance. Access to content should continue to be regulated by other legislation and clearly prohibited in this Bill.

154. The challenge of excluding content is exacerbated by the fact that there is no clear consensus about precisely what constitutes content in the internet age. When telephones were the main generators of communications data, the definition of content was clear: it was the words exchanged over the phone (never saved by the CSP and only accessible if an intercept warrant was granted); the voice message in voicemails (CSPs might have had access to those that were stored on a voicemail platform and had either not been listened to

102 Q 1144

yet, or had been listened to and had been saved for a few days) and in more recent times the text of SMS messages (CSPs might have had access to those that were on an SMS server awaiting delivery to a subscriber, or those that had been delivered to a subscriber, but were still sitting on the server). It was clear to everyone that these were content.

155. With internet based communications the line between content and data is harder to draw. For example, when a person subscribes to a social network they may be given the option to fill in data fields that include their religious views, sexual preferences, favourite TV shows etc. Do these data fields really only include "data"? It is not just social networks that raise this problem. It is also an issue for companies where the provider provides more than communications services. The information these companies hold on their customer management systems may go far beyond what is thought of as communications data although it may have been collected as customer data for non-communications services. Taken to extremes, if a hotel were to be designated as a CSP (because it allows guests to make calls from their bedrooms), then all of the hotel booking information, pillow preferences etc, could fall under the definition of "subscriber data". As discussed in Chapter 4, we received evidence from those that argued that web addresses, even those limited to information before the first "/", were more akin to content than data.

156. The problems inherent in trying to define content make it more important than ever that the legislation clearly defines communications data and the various categories which comprise it. One way to do this is more tightly to define subscriber data as discussed below. Another is explicitly to exclude content from every category of communications data.

The definition of communications data

157. The draft Bill uses the RIPA definition of communications data. The definition has not changed, despite the fact that communications technologies, and thus the types of information held by providers, have significantly evolved. The definition was developed at a time when telephony records were considered to be of more immediate interest to investigators than a person's usage of the internet. The language of the draft Bill is peppered with references to telecommunications technologies. The term 'Telecommunications Operator' is used to cover those that provide internet services

158. Several of our witnesses were concerned about this approach. Vodafone's written evidence stated that "Clearly, taking a pre-internet model and assuming it works in the internet age isn't necessarily going to deliver a workable long-term solution". Mark Hughes from BT made the case that new technologies make it ever more important robustly to define the differences between communications data and content.[103]

159. In relation to a telecommunications operator, service or system (as opposed to a postal operator or service) communications data is defined with reference to three categories: traffic data, use data or subscriber data (see Box 8).

103 Q 434

BOX 8: Definitions of Communications Data in the draft Bill

"Subscriber data" means information (other than traffic or use data) held or obtained by a person providing a telecommunications service about those to whom the service is provided by that person.

"Use data" means information-

1. Which is about the use made by a person –
    a. Of a telecommunications service, or
    b. In connection with the provision to or use by any person of a telecommunications service, or part of a telecommunications system, but
2. Which does not (apart from information falling with paragraph (a) which is traffic data) include any of the contents of a communication.

"**Traffic data**" means data –

a) which is comprised in, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a telecommunication system by means of which the communication is being or may be transmitted, and

b) which—
    i. identifies, or purports to identify, any person, apparatus or location to or from which the communication is or may be transmitted,
    ii. identifies or selects, or purports to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted,
    iii. comprises signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of the communication,
    iv. identifies, or purports to identify, the time at which an event relating to the communication occurs, or
    v. identifies data as comprised in, attached to or logically associated with

160. The definition of subscriber data is particularly problematic because it is a catch-all for information that does not fall into the other two categories. In the telephone age there was a clear and finite amount of data that did not fit the criteria for use or traffic data. In the internet age this is not so clear. This point was made forcefully in the written evidence submitted by JANET:

> "The definition of "communications data" in clauses 28(1) to 28(5) will extend much wider than the normal meaning of that term (and the stated intention of the draft Bill) when it is applied to organisations such as universities, webmail and social network services, all of which appear to be included in the current definition of "telecommunications operator".
>
> "This is because "communications data" is defined in clause 28(1) as the aggregate of "use data", "traffic data" and "subscriber data". Clause 28(5) then defines "subscriber data" as "information (other than traffic data or use data) held or obtained by a person providing a telecommunications service about those to whom the service is provided by that person". In other words "communications data" will comprise all information held by the service provider about the individuals who use the service. In the case of a university or social network this would cover much more than is normally considered subscriber or communications data: for example it would include a student's academic record or a member of staff's personnel file."

161. ISPA agreed:

> " the draft Bill defines 'subscriber data' as "information (other than traffic data or use data) held or obtained by a person providing a telecommunications service about those to whom the service is provided by that person." Social networks often ask their users for information about their gender, religion, relationship status etc. which should not only be considered as very personal information but is also information that is currently not retained for law enforcement purposes."[104]

162. The potentially wide application of the definition of subscriber data is particularly worrying given that this data is considered to be the least intrusive of the three data types. That was the intention when RIPA was drafted and the Regulation of Investigatory Powers (Communications Data) Order 2010[105] reflects this by providing that authorisations in respect of the acquisition of subscriber data can be made in the case of a police force by an inspector whilst authorisations to obtain use and/or traffic data must be made by a superintendent. Clauses 17(2) and (3) of the draft Bill provide an equivalent order-making power which will permit the Secretary of State to provide a lower level of authorisation for subscriber checks than for traffic data checks. As Demos put it:

> "The current legislation—the RIPA 2000—is animated by the basic precept that the more possibly harmful the interception, the fewer agencies should be authorised to access and use the information, the narrower an acceptable justification for such access should be, the tougher the oversight of the process has to be."[106]

104 ISPA written evidence, para 29

105 S.I. 2010/480.This consolidates previous Orders but the position as to acquisition of subscriber data remains unchanged.

106 Demos written evidence

163. If this was the basic precept of RIPA, and continues to be the precept of the draft Bill, then the definition of subscriber data is not fit for purpose.

164. When we visited the law enforcement unit at the Metropolitan Police we had the opportunity to talk to several SPoCs about the communications data requests they see (see appendix 4). It was clear that the information sought under the heading "subscriber data" is information similar to a reverse directory check, it is information that links an individual to an account. Law enforcement is not asking for the capability to see the wide range of data that could potentially fall under the current definition of subscriber data. The drafting of the Bill is thus not reflecting either the needs of law enforcement or the realities of new technologies and it is unnecessarily giving rise to concerns about access to content.

165. If the definitions of subscriber, use and traffic data are in need of review, what should be the way forward? First, we refer back to the lack of consultation before the publication of this draft Bill (see paragraphs 46-60). Industry, technical experts, lawyers and civil liberties groups could all provide valuable input into a revised definition but they were not given the chance to do so. A consultation on the particular challenge of defining communications data is needed.

166. Demos made a further suggestion about how a revision of definitions could be approached:

> "...we believe the following inter alia principles could be useful to determine and measure the degree of privacy intrusion of various communications data collected and used, and thus the level at which it should be authorised, the list of acceptable purposes, and appropriate level of oversight:

- Public attitudes about the extent to which a certain type of communications data is private, and level, and therefore how intrusive data collection is
- The risk of identifying details of an individual's life, behaviour, beliefs, that they would reasonably consider personal
- The risk of data being misused (i.e. used in a way not set out by the legislation) or accessed by third parties, either intentionally or not
- The context in which the data are being used (i.e. whether to create aggregated, anonymous data sets or targeted at individuals)."[107]

167. **The language of RIPA is out of date and should not be used as the basis of new legislation. The Bill should be re-drafted with new definitions of communications data. The challenge will lie in creating definitions that will stand the test of time. There should be an urgent consultation with industry on changing the definitions and making them relevant to the year 2012.**

168. **The definitions of use, subscriber and traffic data are particularly problematic. Subscriber data should not be a catch-all for data that does not meet the other definitions. Currently the definition of subscriber data could be read to cover all sorts of data that social networks and other services keep on their customers which can be**

107 Demos, supplementary written evidence

highly personal and is not traditionally thought of as communications data. A new definition of subscriber data is needed that simply covers the basic subscriber checks that are the most commonly used. How to define subscriber data should be a key element of the consultation, but the evidence we have received leads us to suggest that the definition should include checks on the name, date of birth, addresses and other contact information held on the subscriber to a communication service; for each service the customer's unique ID (e.g. mobile number, e-mail address or username); the activation, suspension and termination dates of an account and payment and billing information.

169. **A new hierarchy of data types needs to be developed. Data should be divided into categories that reflect how intrusive each type of data is. The following principles could be useful to determine and measure the degree of privacy intrusion of communications data: public attitudes about the extent to which a certain type of communications data is private; the risk of identifying details of an individual's life, behaviour, beliefs, that they would reasonably consider personal; the risk of data being misused (i.e. used in a way not set out by the legislation) or accessed by third parties, either intentionally or not.**

170. **It is imperative that everything is done to make clear that content cannot be requested under the provisions of this legislation. Content is not defined in the draft Bill. Although it may not be possible to define content clearly beyond the fact that it is the "what" of a communication, it is nevertheless important that the content should be expressly excluded from all categories of communications data.**

The authorisation process

171. Requests to access communications data are currently subject to an internal authorisation process which was described in some detail in Chapter 2. To briefly recap: every application has to be authorised by a Designated Senior Officer (DSO) from the organisation that is making the request. Before the application reaches the DSO it is channelled through a Single Point of Contact (SPoC) who is a trained expert, independent of the investigation, who will advise the applicant and the DSO on whether the application is necessary and proportionate, what collateral damage may result and whether the communications data sought is likely to be available.

172. On our visit to the Metropolitan Police Central Intelligence Unit we saw in action the system which covers the whole of the Metropolitan Police.[108] We talked to some of the large number of SPoCs, and were impressed by the high level of their training and the thoroughness with which they considered each and every application. While SPoCs do not authorise applications themselves we saw examples where they referred applications back to the investigating officer on the grounds that additional information was required before a DSO could consider authorisation. We also spoke to several DSOs who explained the detailed advice they receive from the SPoCs on the necessity and proportionality of each application. Later in our inquiry we took evidence from Detective Superintendent Steve Higgins who is in charge of communications data training at the National Policing Improvement Agency. He stated that SPoC training was constantly being reviewed and

108 See Appendix 4.

updated[109] and that SPoCs are trained to challenge more senior officers if the communications data requests they submit are inappropriate[110].

173. We also saw the system from the other end when we visited Everything Everywhere, one of the major recipients of applications for communications data. They told us that the requests which reached them almost invariably had been carefully considered, and satisfied the statutory requirements.[111] Virgin Media's written evidence stated: "The current regime has strengths, particularly the Single Point of Contact System, which provides an important framework for the relationship between law enforcement authorities and CSPs." ISPA said: "We believe that the current regime performs fairly well, in particular the dedicated expertise in the Single Point of Contact System, which has provided for an effective means of structuring the relationship between law enforcement authorities and CSPs."[112]

174. Many police forces make frequent use of the SPoC system, as do some other law enforcement agencies. Most other designated authorities, in particular local authorities, use it infrequently or only rarely by virtue of the fact that they are not frequent users of communications data. Inevitably the applicants are less familiar with the procedure, the SPoCs less well trained and less experienced, and the DSOs act in that capacity less often. This heightens the risk that errors may creep in. Such risk can however be mitigated by the pooling of expertise. Some of the smaller police forces have already joined together with neighbouring forces to share their SPoC expertise. The National Anti-Fraud Network (NAFN) provides SPoC services for many local authorities. NAFN is an unincorporated, not for profit organisation created and managed by local authorities to provide specialist data and intelligence services. The IoCC's inspection team has reported that "The Accredited SPoCs at NAFN are providing an excellent service".[113]

175. Some of our witnesses suggested that the internal authorisation procedure was not sufficiently independent or robust and they argued that all or most applications for communications data should be subject to judicial approval. For example Justice stated that:

> "JUSTICE considers that the administrative authorisation procedure provided for in clauses 9 and 10 provide for inadequate independent scrutiny of the need for access to data. These provisions are largely modelled on RIPA. In Freedom from Suspicion, we explained our view that prior judicial approval should be the default authorisation mechanism for most surveillance activities, including access to communications data. While it is no doubt true that senior members of organisations are typically well-placed to supervise the operational decisions of their subordinates, and more mindful of their ultimate accountability to the public, it is also clear that senior and junior members of the same organisation will inevitably share an interest in achieving the necessary results."[114]

109 Q 1108

110 Q 1113

111 See Appendix 5.

112 ISPA written evidence

113 Annual report of the IoCC 2011, July 2012, HC 496, page 39.

114 JUSTICE, written evidence, paragraph 28

176. Liberty agreed:

> "Liberty maintains that even if a designated officer is not directly involved in an investigation it is entirely unacceptable for public authorities to be able to self-authorise access to revealing personal data, particularly when the access regime is so broadly framed. Considerations of necessity and proportionality should be assessed by a member of the judiciary who will be both independent and adept at conducting the Article 8 balancing exercise. We do not seek to impugn the integrity [of] senior employees of our law enforcement agencies, but rather point out the reality that their primary concern will relate to the operational capacity of their agency. This is a matter of organisation culture and is perfectly understandable, but it is also a reality which mitigates in favour of independent third party authorisation."[115]

177. We explained in paragraph 135 how, following some high profile cases where local authorities misused communications data, the law was changed on 1 November so that authorisation for a local authority to access communications data now needs the approval of a magistrate. Civil liberties groups called for this model to be extended to all public authorities.

178. We understand the principles behind these views but we are not convinced that in reality a magistrate would provide a tougher authorisation test that the current system. Magistrates would not have access to the SPoC expertise to advise them on the necessity and proportionality of each request. There are also practical considerations; the sheer volume of communications data requests would place a huge burden on the judiciary and a judicial authorisation process would lead to delays in access to communications data. Such delays could prove harmful to live investigations. It is our view that the current internal authorisation procedure is the right model. Having said that, there are ways that the internal authorisation model could be strengthened.

179. The first step to strengthening the current model is to ensure that the advice of an expert SPoC is always sought. The SPoC system is an integral part of the RIPA request process. The role is referred to in the Code of Practice for the Acquisition and Disclosure of Communications Data (a statutory code which was made pursuant to section 71(3) RIPA, brought into force by the Regulation of Investigatory Powers (Acquisition and Disclosure of Communications Data: Code of Practice) Order 2007).[116] The Code sets out what amounts to best practice which authorities are required to have regard to when seeking communications data. The failure to adhere to the Code of Practice would be taken into account by a court in any proceedings against an authority for misuse of its powers to obtain data. It is our view that the SPoC service should be made a statutory requirement for all authorities which have access to communications data.

180. The second step to strengthening the current model is to encourage more pooling of SPoC resources along the lines of the NAFN model. It should be obligatory that all local authorities use the NAFN service and that other infrequent users of communications data also use a centralised service.

115 Liberty written evidence, paragraph 73

116 SI 2007/2197

181. The third step is to strengthen the inspection regime. The public do not have confidence in the internal authorisation model but if the inspections of the IoCC were more thorough and the reports of the inspectors were more detailed then this could build confidence.

182. Representatives from the police were keen that more should be done to demonstrate how robust the current system is. Detective Superintendent Allan Lyon told us "I think the inspection process, which is independent and separate from the police, may be an opportunity to develop some sort of public communication programme that can reassure the public that Greater Manchester Police treats this particular sensitive tactic with the utmost respect and we deal with it in a very lawful and transparent way".[117] Sir Peter Fahy agreed "I think it is frustrating that the public and some of the commentators do not seem to understand. I regard it very, very seriously, because this is an important capability. If there is any concern whatsoever from the public that we are using this inappropriately, that would be a huge damage to policing and a huge damage to victims of crime."[118]

183. The role of the Interception of Communications Commissioner and his inspection regime are discussed in greater detail in the next section.

184. **The SPoC process should be enshrined in primary legislation. A specialist centralised SPoC service should be established modelled on the National Anti-Fraud Network service which currently offers SPoC expertise to local authorities. The Home Office should consider allowing police forces to bid to run this service. This new service should be established by statute, and all local authorities and other infrequent users of communications data should be required to obtain advice from this service.**

185. **In the case of local authorities it should be possible for magistrates to cope with the volume of work involved in approving applications for authorisation. But we believe that if our recommendations are accepted and incorporated into the Bill, they will provide a stronger authorisation test than magistrates can.**

186. **Although approval by magistrates of local authority authorisations is a very recent change in the law, we think that if our recommendations are implemented it will be unnecessary to continue with different arrangements applying only to local authorities.**

The Interception of Communications Commissioner

187. An additional safeguard was the creation by section 57 of RIPA of the office of Interception of Communications Commissioner (IoCC), one of whose duties is "to keep under review … the exercise and performance, by the persons on whom they are conferred or imposed, of the powers and duties conferred or imposed by or under Chapter II of Part I [of RIPA]". In other words, he inspects the working of the system for access to communications data to make sure that it is done entirely in accordance with the statute, and makes recommendations for improvement when errors occur. The purpose is to reassure the public that intrusion is kept to a minimum and their privacy is respected as far as is consistent with the aims of the legislation.

117 Q 1118

118 Q 1120

188. This is only one of the duties of the IoCC. He also has to keep under review the Secretary of State's use of interception warrants, the investigation of electronic data protected by encryption, and the adequacy of the safeguards; and he has undertaken to oversee the interception of the communications of prisoners. Sir Paul Kennedy, the current Commissioner,[119] gave us written and oral evidence. In addition, his annual report for 2011[120] contains a great deal of useful material and is more comprehensive than earlier reports.

189. The annual report explains that where a public authority has submitted only a small number of communications data applications "it is likely that they will all be examined". Public authorities which make only a handful of requests every year—or perhaps only in some years—inevitably have less experience of the system and are more likely to make errors.[121] We do not know how a "small number" is defined, or how likely it is that they will be examined. The example Sir Paul gave was that "when my inspectors go to a small user who has made seven applications—and that would be quite a lot sometimes—for data over the last two years, they inspect them all, so there is no question there of any type of sampling."[122] We would prefer to be assured that in the case of every authority submitting fewer than, say, 100 applications a year, they were all routinely examined.

190. For the remainder of the half million requests made during 2011 the inspectors can only select a random sample and check that they have been dealt with strictly in accordance with the Act and the Code of Practice. It is clear from the annual report that inspections of the main law enforcement authorities find only a very small proportion of errors—though a small proportion of half a million is still a significant number. And, as we have shown in Chapter 4, the proportion of errors made by local authorities is twenty times the average of other public authorities.

191. It is not only the public authorities which make errors. The annual report shows that in two cases a CSP disclosed incorrect data in response to a request, the police took action on the basis of this data, and members of the public were wrongly detained and accused of crimes.

192. We think it a fair summary of Sir Paul's evidence to say that in his view the system is broadly working well, that comparatively few errors are made, that only a few of these are serious, and that his inspectors do a thorough job through which they can discover where the system is failing, and make recommendations to put this right which are followed. However, one of the purposes of the inspections is to reassure the public, and the evidence is that they are not reassured. The written evidence of Caspar Bowden contains lengthy and detailed criticisms of the role of the IoCC and the way his role is discharged. The view of Angela Patrick, the Human Rights Officer of JUSTICE, was that the inspectors were looking mainly at factual compliance, but that "the Commissioner either does not see looking at necessity and proportionality as a core part of his role or, alternatively, they [the

119 He will be retiring at the end of 2012. His successor will be Sir Anthony May, also a former Lord Justice of Appeal.

120 July 2012, HC 296.

121 The Business Cases for access by public authorities show, for example, that in the last 3 years the IPCC has made 42 requests, the OFT has made 28 requests, HSE has made 26 requests, the Criminal Cases Review Commission has made 2 requests, while the Food Standards Agency and the Pensions Regulator have made none.

122 Q 662

inspectors] simply do not have the expertise or the resources to be able to apply that kind of balance."[123]

193. The IoCC does not explain in his annual report how his team assess necessity and proportionality. Sir Paul told us that in his view it was not possible to develop a formula, but he believed it was something that is easy to assess when looking at individual cases.[124] Several civil liberties campaigners were concerned about this apparent lack of transparency. Caspar Bowden asked: "What does the IoCC consider "necessary and proportionate"? Under the UK regime, almost all jurisprudence about interception and communications data takes place invisibly within the cranium of the IoCC, and almost nowhere else".[125] The Open Rights Group stated that the lack of concrete information illustrating what is and is not judged acceptable raises questions about the spirit of ECHR compliance.[126]

194. We accept that these concepts are not easy to define. We believe that it would at the very least be helpful if the IoCC, rather than simply saying in his annual report that "my inspectors seek to ensure … that the disclosure required was necessary and proportionate to the task in hand", could give examples of where they have thought that this test was satisfied, and where they believe it was not.

195. For these inspections the IoCC is assisted by a chief inspector, five inspectors and two administrative staff, who also have to support the IoCC in his other duties. Section 57(7) of RIPA requires the Secretary of State to provide the Commissioner with "such staff as are sufficient to make sure that the Commissioner is able properly to carry out his functions". Clearly, there is no way in which a staff of six inspectors can scrutinise the exercise and performance of the system for accessing communications data in a way which will reassure the public. The numbers must be increased at least to a level where they can fully scrutinise each public authority every year, and carry out a full scrutiny of those that only rarely make use of the system.

196. **The IoCC should carry out a full review of each of the large users of communications data every year. While sampling is acceptable as a way of dealing with large users, the requests of users making fewer than 100 applications in a year should be checked individually. The annual report of the IoCC should include more detail, including statistics, about the performance of each public authority and the criteria against which judgments are made about performance. It should analyse how many communications data requests are made for each permitted purpose. For this the IoCC will need substantial additional resources, both as to numbers and as to technical expertise. There should be full consultation with him on this. His role should be given more publicity.**

197. **The IoCC's brief should explicitly cover the need to provide advice and guidance on proportionality and necessity, and there should be rigorous testing of, and reporting on, the proportionality and necessity of requests made.**

123 Q 241

124 Q 668

125 Caspar Bowden written evidence

126 Open Rights Group written evidence

198. Sir Paul Kennedy told us that he had yet to be given enough information about the Request Filter fully to understand his new responsibilities for operating it, but that he expected it would need new expertise within his office:

> "So far as the second part of what is envisaged is concerned, that is the filtering side of the operation, I think—and I am only guessing here because we have not yet got anything in place against which you can run the tests—that will require a degree of expertise that at the moment we do not have in-house. For that purpose it may well be necessary to recruit someone with an IT background, either on a full-time or a part-time or a consultancy basis, to discharge the obligation that is placed upon the commissioner by the Bill if it becomes law."[127]

199. **The IoCC will be key to public confidence in the Request Filter. The IoCC will need the necessary expertise properly to examine the operation of the Request Filter. He will have to report on the scale of searches via the Request Filter and rigorously test the necessity and proportionality of requests put to the Filter. All this information should be included in the public section of his annual report so that if there are any signs that the Filter is resulting in more intrusive requests Parliament can review the legislation.**

The Information Commissioner

200. As in the case of the IoCC, oversight by the Information Commissioner is intended to be one of the safeguards which ensure that the powers under the draft Bill are not misused or abused. The only provision of the draft Bill imposing obligations on the Information Commissioner is clause 22(5):

> "(5) The Information Commissioner must keep under review the operation of—
>
> (a) sections 3 and 6 of this Act, and
>
> (b) any provisions in an order under section 1 of this Act which relate to the security of communications data held by telecommunications operators."

201. Clause 3 imposes on telecommunications operators a duty to secure the quality, security and protection of data, and to protect its integrity; clause 6 provides for the destruction of data "in such a way that it can never be retrieved—a problem we deal with later in this chapter. Clause 1 we have dealt with in the previous chapter.

202. Christopher Graham, the Information Commissioner, had this to say about his duties under paragraph (a): "It is not clear what the duty to 'keep under review' the operation of sections 3 and 6 is meant to achieve in practice ... If the intention is for the Information Commissioner to play an active role in inspecting and then assessing whether safeguards are being adhered to in practice then this wording falls short of achieving the desired objective. The Information Commissioner's existing powers to assess processing are also insufficient … [they] fall short of the powers needed to undertake ongoing, effective and proactive scrutiny of a telecommunications operator's activities ... It may be possible, with the close co-operation of telecommunications operators and other relevant regulators, to

127 Q 672

build up an impression of whether the provisions are being adhered to; but that might only be of partial and limited value given the complex technical nature of the proposals. It is hard to see that it would provide the level of safeguard envisaged by those promoting this legislation…"[128] It is clear that the Information Commissioner could not monitor compliance with clauses 3 and 6 in the case of data kept overseas by providers not based in the United Kingdom.

203. He was similarly perplexed about what he was supposed to do in relation to clause 1, and how: "It is not clear whether the details of the operators to whom these notices are issued will be in the public domain or even available to the Information Commissioner for his supervisory activities. Not only does the Information Commissioner need the powers over telecommunications operators and the resources necessary to provide the oversight he is expected to deliver, he also needs a right to receive relevant information from the Secretary of State."[129] Notices under clause 1 will be secret.[130] Whether they will be shown to the Information Commissioner is not clear to him or to us.

204. We asked Mr Graham what the Home Office had told him about these proposed additional duties. He replied:

> "I have not heard from the Home Office whether this is merely an expression of the responsibilities that the Information Commissioner has anyway in relation to data protection or whether something new and extra is envisaged, because if one is going to be part of a framework of reassurance where safeguards are built into the Bill, frankly it has to be more than aspiration. I am told that I am to keep things under review, but I would like to know how and with what."[131]

205. A little later he added:

> "What I have not had is any discussions with the Home Office about how the regime is expected to work. I did not see the Bill. I saw the draft clauses that concern the Information Commissioner I think the day before, possibly the week before. I have had one telephone call with the Minister responsible since, and that is it."[132]

206. We found it hard to understand how additional duties could be imposed on the Information Commissioner without first consulting him, asking him what duties he thought sensible and feasible, whether he would be able to comply with them, and what additional resources he might need to do so. We put this to Home Office officials on 24 October, and Charles Farr replied:

> "The Information Commissioner had seen the draft clauses of the Bill which affected him in advance. He had a meeting with the Minister; he had three hours with Richard going through the detail of the legislation."[133]

128 Information Commissioner's written evidence, paragraphs 16-19

129 Information Commissioner's supplementary written evidence, 6 November 2012.

130 Peter Hill, Q 917

131 Q 694

132 Q 696

133 Q 859

207. As in the case of the consultation with the CSPs, which we discussed in the preceding chapter, this evidence appeared to contradict what the Information Commissioner had told us. Subsequently however the Home Office agreed that the reference to a "meeting" with the Minister was an error; this was in fact a phone call following the publication of the draft Bill. As to the draft clauses affecting him, the Information Commissioner has told us in a letter of 6 November that he asked on 23 May to see them in advance of a meeting on 31 May; his request was refused, and it was only at that meeting that he was given a copy of those clauses. He was sent a copy of the draft Bill the day before it was published.

208. In a note sent to us subsequently the Home Office suggested that the Information Commissioner's duties under the draft Bill were little more than an extension of his duties in relation to the Data Retention Directive under Regulation 6(2) of the Data Retention (EC Directive) Regulations 2009, which states: "It is the duty of the Information Commissioner, as the Supervisory Authority designated for the purposes of Article 9 of the Data Retention Directive, to monitor the application of the provisions of these Regulations with respect to the security of stored data." The Information Commissioner replied that his duties under the Bill would be "on a different scale" and "more challenging". He noted in particular the new requirement to monitor the destruction of data in such a way that "it can never be retrieved", which in his view will involve extensive work needing additional specialist technical expertise.[134]

209. The Information Commissioner told us several times that he would need additional resources for any duties imposed on him, and that he had not been consulted on this.[135] On 24 October, Charles Farr said: "We have consulted with him. We believe that the sum is about £150,000, and that it is affordable as part of the £1.8 billion."[136] In his letter of 6 November the Mr Graham said that the figure of "about £150,000" was one he quoted in his phone call to the Minister on 14 June. He added: "There has been no consultation at all on resources. There has been no discussion around a business plan, either the ICO's or the Home Office's. The ICO has not been asked for a business plan and has not submitted one, for the reasons I gave in my evidence."

210. In a note submitted to us on 9 November, the Home Office said: "The Information Commissioner has provided an estimate of £150,000 per year in additional costs for meeting his responsibilities under the legislation. We are discussing with him how he envisages carrying out his responsibilities (which are largely the same as today) and the business case for the additional costs. As with the Interception Commissioner, we will meet any legitimate costs in meeting his responsibilities under the legislation."

211. These discussions would have been better conducted at the beginning of the year rather than the end. What is clear to us is that the Government has chosen to include in a draft Bill which had a very long gestation a clause imposing on the Information Commissioner additional duties, and that prior to the publication of the Bill there was no consultation with him about those duties, about the information he would need to carry them out, about whether it would in fact be possible for him to undertake those duties, about whether he would need further powers, and about what extra resources he might

134 Information Commissioner's supplementary written evidence, 6 November 2012.

135 QQ 694-700

136 Q 893

need. If they hoped that, by inserting this clause in this way, they would be providing an additional safeguard which might allay concerns about the draft Bill, we can only say that they were mistaken.

212. **Clause 22(5) should be reviewed. If the Government believe that additional safeguards can be provided by the Information Commissioner, they should undertake detailed discussions with him as to what such safeguards might be, how they might be undertaken, and what additional powers and resources he might need. The Bill should make clear that the Information Commissioner will need to be shown all notices issued under clause 1.**

Other surveillance commissioners

213. The Information Commissioner sent us what he described as a draft of a Surveillance Road Map.[137] It sets out all the United Kingdom surveillance legislation, and lists the roles and responsibilities of the Commissioners who regulate surveillance in the United Kingdom:

- Information Commissioner
- Interception of Communications Commissioner
- Chief Surveillance Commissioner, overseeing the use of covert surveillance, so that his role overlaps to some extent with oversight of intrusive and directed surveillance under RIPA, and with the Information Commissioner's powers under the Data Protection Act 1998;
- Intelligence Services Commissioner;
- Investigatory Powers Tribunal, which can hear complaints from individuals about interference under RIPA by public bodies;
- Investigatory Powers Commissioner for Northern Ireland;
- Surveillance Camera Commissioner and Biometric Commissioner, both appointed under the Protection of Freedoms Act 2012.

214. The Surveillance Road Map sets out the circumstances where individuals can complain, and to whom, and the gaps that still need to be filled by secondary legislation (in accordance with the Protection of Freedoms Act).

215. The Information Commissioner referred to the conclusion of the House of Commons Home Affairs Committee "that there ought to be either a single privacy commissioner or a sort of primus inter pares".[138] He made the point that his responsibilities extend beyond data protection to freedom of information, and so relate to both privacy and open government. For this reason he asserted that his responsibilities should not be altered. However, the seven other Commissioners have been set up under a variety of statutes, and it does not seem that much thought has been given to whether any new duties could be

137 Not submitted as evidence to our inquiry and so not published with the written evidence.

138 Q 694

carried out by a Commissioner already in existence, without creating yet another. This does not strictly fall within our consideration of the draft Bill, but we suggest that some thought should be given to a merger of their powers and responsibilities.

216. **Work should be done to rationalise the number of commissioners with responsibility for different areas of surveillance. This work should aim to simplify the situation and make it easier for the public to understand, while ensuring that all surveillance powers are subject to rigorous oversight. Consideration should be given to a new unified Surveillance Commission reporting to parliament with multi-skilled investigators and human rights and computer experts.**

Security and destruction of data

217. The inevitable consequence of the draft Bill is that a larger quantity of communications data will be stored relating to a larger number of people. This makes it ever more important to ensure that data can be stored securely and disposed of permanently.

218. The draft Bill addresses storage and destruction in several ways. Clause 1 allows a notice served on a CSP to provide for the processing, retention or destruction of data. clause 6 provides for the destruction of communications data at the end of the retention period. The data must be destroyed in such a way that it can never be retrieved. The deletion of data must take place within a month of the end of the retention period.

219. Several of our witnesses questioned whether it was possible to guarantee the safe storage and permanent destruction of data. We took evidence from Glynn Wintle, an IT security expert paid by companies to test the security of their systems, who stated "From my personal experience of trying to break into systems, you may find one person who does a really good job. If you gave me 10 companies and said, "Pick one of them", I know that I am going to get into one of them".[139] Professor Sadie Creese questioned whether CSPs could guarantee that they would be able to identify where data was physically located in order to ensure it was stored and destroyed correctly: "you may find that behind closed doors people in their evidence will be willing to tell you that they do not always know where everything is, do not know where some of this digital stuff has moved to, and cannot absolutely guarantee to you that it has been "destroyed", to use the language of the Bill."[140] In fact none of the CSPs were willing to admit to this but Vodafone did raise concerns about the requirement to destroy data so that it can never be retrieved: "We also have concerns about the requirement for an operator to destroy data "in such a way that it can never be retrieved." "Never" is an unrealistic requirement, because we are not in a position to determine the state of the art in the future".[141]

220. Another concern was the cost of storage and destruction. Glynn Wintle raised this: "I was quite surprised that the Home Office did not talk about the cost of destroying data when they talked about costs; they said that their biggest costs were going to be on training. Getting rid securely of all that data—destroying it—is a very nontrivial thing to try to do,

139 Q 361

140 Q 360

141 Vodafone written evidence

especially in the volumes that they will be dealing with. Securing this data, likewise, is going to be an interesting problem".[142]

221. One of the safeguards in the draft Bill is that clause 22(5) places a duty on the Information Commissioner to keep under review the operation of provisions relating to data security and the destruction of data. Whether or not this safeguard will be effective will depend on the powers and resources that will be given to the Information Commissioner as discussed in the previous section. Christopher Graham told us that in relation to this specific duty "The first thing I would have to do would be to employ specialist staff to complete this work, given the complex and technical nature of what is being asked of us. I will certainly need the compulsory audit powers under the Data Protection Act to be able to take on that work. These are all conversations that we need to have, but obviously the public will need reassurance that the obligation to delete will be honoured and there will not be a temptation on the part of communications service providers having been asked to hang on to material that they would not have hung on to in any other circumstances to do something with it".[143] He also called into question whether he would be able to ensure that data can never be retrieved:

> "The overarching concerns of the Information Commissioner are how achievable the destruction envisaged in the Bill is in practice and how he can keep under review the operation of these requirements short of a power to inspect the relevant information systems of operators to actually check that data is no longer being retained.
>
> Further, even if the Information Commissioner had inspection and/or audit powers it would still be technically and practically challenging for him to establish that data that have supposedly been destroyed 'can never be retrieved'."

222. **Security of data can never be completely guaranteed; the higher the level of security, the greater the cost. This legislation will require more to be stored, and more to be stored overseas. It therefore increases the risk of security breaches.**

223. **We consider that the Home Office's cost estimates may underestimate the cost of security and destruction. Since the cost of security and destruction will ultimately be borne by the taxpayer, the Home Office will have to carry out a careful cost/benefit analysis and obtain advice and assurances from a wider body of experts than the companies that stand to earn money from devising secure storage solutions.**

Offence of misuse of communications data by a public authority

224. There is already a huge quantity of highly personal data collected and potentially accessible by a large number of individuals. The draft Bill would greatly increase opportunities for misuse and abuse. The public needs to be reassured that appropriate legislation is in place to provide both a deterrent and a punishment.

225. We agree with the Home Office that there is no need for criminal offences to punish minor administrative errors made by officials in public authorities while seeking to acquire communications data. Where appropriate, disciplinary action should suffice. But wilful or

142 Q 361

143 Q 700

reckless conduct is another matter. The Home Office believes that there are already enough offences on the statute book to deal with this, including:

- Unauthorised access to computer material, contrary to section 1 of the Computer Misuse Act 1990, which carries a maximum sentence of two years' imprisonment;
- Unauthorised access with intent to commit another offence, such as fraud, contrary to section 2 of the Computer Misuse Act 1990, which carries a maximum sentence of five years' imprisonment;
- Knowingly or recklessly obtaining, disclosing or procuring the disclosure of personal data without the consent of the data controller under section 55 of the Data Protection Act 1998, which carries a maximum penalty of an unlimited fine but not, at present, a custodial sentence;
- The common law offence of misconduct in public office. It is committed when the office holder wilfully acts (or fails to act) in a way that he knows is wrong and is calculated to injure the public interest. The maximum penalty for this offence is life imprisonment.

226. An unlimited fine for an offence under section 55 of the Data Protection Act 1998 is on the face of it a severe penalty; but the Information Commissioner told us that in practice it is "not a very scary provision".[144] In evidence to the House of Commons Justice Committee on 13 September 2011 he explained that the going rate was a fine of £100 to £150, and that this was "simply not a deterrent".[145] But the remedy is on the statute book, in the shape of section 77 of the Criminal Justice and Immigration Act 2008.[146] Under section 77 the Secretary of State has power by order to increase the penalty to allow a custodial penalty. Mr Graham told us: "I have spent three years urging Parliamentary committees to commence sections 77 and 78 of the Criminal Justice and Immigration Act because it contains the power to impose a penalty up to and including prison in serious offences."[147] **The House of Commons Justice Committee recommended that the power under section 77 of the Criminal Justice and Immigration Act 2008 should be exercised "without further delay".**[148] **Nearly a year later the Home Affairs Committee reached the same conclusion.**[149] **We agree with the Information Commissioner and with both these Committees that this power to allow custodial sentences to be imposed in appropriate cases should be exercised without delay.**

227. It has been suggested that the Government may be awaiting the outcome of Lord Justice Leveson's inquiry. Section 78 of the 2008 Act, which has not been brought into force, would provide a specific defence for journalists in the case of an offence under section 55 of the Data Protection Act, and the two provisions are therefore connected. Unless the report of the Leveson inquiry, which will be published just after we agree this

144 Q 695

145 http://www.publications.parliament.uk/pa/cm201012/cmselect/cmjust/1473/11091302.htm

146 Section 77 came into force on the passing of the Act: see section 153(1).

147 Q 709

148 Ninth report, session 2010-2012, paragraph 9.

149 Fourth report, session 2012-2013, paragraph 47.

report, contains recommendations to the contrary, we see no reason for further delay in the Secretary of State exercising her powers under section 77 of the 2008 Act.

228. Even once these powers have been exercised, we believe there is still a need for a specific offence aimed at wilful or reckless conduct in relation to communication data. We cannot tell whether the offences listed at paragraph 224 would cover all such conduct, or whether the courts would deal with such offences with sufficient severity. We believe the public would be reassured to know that there was a specific offence on the statute book which might act as a deterrent for such conduct, and a punishment if and when it took place.

229. **The draft Bill should provide for wilful or reckless misuse of communications data to be a specific offence punishable in appropriate cases by imprisonment.**

6 Jurisdictional issues

Requests addressed to overseas CSPs

230. Legislation passed by the United Kingdom Parliament does not have direct effect outside the jurisdiction. This raises particular issues where, as here, the legislation relates to communications with a global reach. Many CSPs, whether based in the United Kingdom or overseas, operate within and outside the jurisdiction.

231. The terms in which RIPA is drafted appear to impose no limits on the telecommunications operators which may be required to disclose communications data, as long as they operate in the United Kingdom is does not matter where they may be based. The reality is rather different. If the CSP is based outside the jurisdiction only two courses are available to UK authorities requesting the data. The first is to rely on the goodwill of the CSP, bolstered by the fact that because they are doing business in the United Kingdom they have an incentive to cooperate. The second is to rely on Mutual Legal Assistance Treaties, the avenue by which the judicial authorities of one State can request the assistance of those in another State. We look at this more fully at later in this chapter.

232. The goodwill is not lacking, as was demonstrated by the evidence we received from a number of overseas operators, including Hotmail, Yahoo!, Facebook and Twitter. All offer services to customers in the United Kingdom through overseas operations. A number of them referred to their existing relationship with the UK law enforcement authorities and the Home Office and to the way in which they presently deal with RIPA requests. Stephen Collins, head of EU Policy, Microsoft when representing Hotmail, referred to the "extremely cooperative professional relationship" which presently exists between Hotmail and UK law enforcement agencies. He explained that in dealing with RIPA requests, Hotmail relies "a lot on so-called voluntary compliance with RIPA as it stands at the moment, in accordance with US, Irish and Luxembourg law".[150] Sarah Hunter, head of UK Public Policy at Google, explained that Google presently has a number of ways to enable law enforcement agencies to access data, including a 24 hour emergency procedure where there is an immediate risk to life. Google (like Microsoft) voluntarily complies with RIPA where possible[151] and encourages use of MLAT procedures in other instances.[152] Colin Crowell, head of Global Public Policy at Twitter, stated that Twitter's policy is, once law enforcement agencies inform Twitter that they are seeking evidence, to preserve it until the agencies go through the legal process to obtain it.[153] Simon Milner explained that Facebook has a Dublin based team handling standard requests from the United Kingdom authorities with a dedicated team in California handling emergency requests, and that United Kingdom law enforcement agencies have apparently indicated to Facebook that they are very happy with the relationship and turnaround times.[154]

150 Q 557

151 Q 568

152 Q 558

153 Q 656

154 Q 627

233. These comments are indicative of a generally cooperative working relationship between overseas CSPs and United Kingdom law enforcement agencies, with CSPs trying to respond to RIPA requests while not recognising them as imposing legally enforceable obligations on them. But we stress that cooperation has to come from both sides. The relationship was well summed up by Stephen Collins:

> "We are operating in good faith with the UK authorities, but we have no obligation to do so. We are doing this because we think it is the right thing to do. If that good faith is abused, we would have to think much more carefully about that co-operation." [155]

234. Nevertheless there are problems. Overseas CSPs will not always disclose communications data even when UK law enforcement judge it to be important. On our visit to the Metropolitan Police we were told of a case of serious online harassment which could not be pursued because the overseas provider who held the necessary data would not release it. The Met told us that there is an increasing problem of harassment on social media which they cannot properly investigate.[156] Another problem is that operators based outside the European Union have no obligation to retain data, nor will they normally do so if they have no business purpose for it. Overseas CSPs are not always prepared to disclose any communications data which they hold. Charles Farr emphasised that there is a dialogue with overseas CSPs and co-operative and collaborative relationships[157] and a "consistent theme of discussion, coordination and cooperation",[158] which leads to the provision of considerable amounts of communications data—up to 75% of what is requested.[159] However, he also explained that there are CSPs based in hostile States which have no interest in creating a co-operative working relationship.[160] In these circumstances data is difficult to obtain.

235. Two elements of the draft Bill are designed to address these problems. First, it would enable the Home Secretary to request a communications provider to retain data, even when the provider has no business reason to do so and where it may be offering services in the United Kingdom from overseas.[161] Secondly, it would enable the Home Secretary to require United Kingdom CSPs to access and retain third party data crossing their networks with a view to communications data being accessible where an overseas CSP does not comply with any notice served on it to retain or disclose data. The third party data provisions are addressed in Chapter 4.

236. We asked Home Office officials how they envisaged the draft Bill would impact on CSPs based overseas. Charles Farr explained:

> "...the obligations do apply to overseas providers and in the event, which I regard as unlikely, that co-operation was not possible, an enforcement route would be open to

155 Q 594

156 See appendix 4

157 Q 48

158 Q 930

159 Ibid.

160 Ibid.

161 "Overseas" in this context means from outside the EU; CSPs in the EU already have an obligation to retain data under the various laws of the Member States implementing the Data Retention Directive.

> Ministers, if they chose to exercise it, through civil action. This would apply as much to overseas providers as to domestic providers. I emphasise that is not the purpose of this legislation. The purpose is to facilitate a collaborative, co-operative relationship, building on the relationships that we have already." [162]

237. Mr Farr also referred to the need for a mandate to require the retention of data not needed for business purposes, and a corresponding power to pay CSPs (including those overseas) for the extra costs incurred.[163] In relation to the collection of third party data from United Kingdom based networks, Mr Farr said that he would not want to "go down the route of collecting third party data from a network here without the collaboration of the service provider," and that he had described it to United Kingdom CSPs as an "*in extremis* power". He went on to explain:

> "I would draw a distinction between our dealings with major UK CSPs and our dealings with smaller niche companies from potentially hostile States. I can imagine that any government may wish to have in its back pocket a power to draw data off a UK network, where a CSP in a hostile State is unwilling to provide it and is not even interested in establishing a cooperative relationship. I think that it is in that sort of context that we envisage using DPI probes, and certainly not, if we can possibly avoid it, in the context of the major CSPs." [164]

238. We referred in paragraph 231to the cooperative attitude of the overseas operators who gave evidence to us. Some of them did have concerns about the developments proposed in the draft Bill. For Hotmail, Stephen Collins found it "perplexing" to be faced with a Bill with "such broad ramifications" and not to be told by any of the agencies with which Hotmail works that there is a problem, and what that problem is.[165] There is a risk that if they are not treated openly and frankly, that cooperation may be jeopardised.

239. All the overseas CSPs which gave evidence to us had major concerns about the jurisdictional issues, and in particular about overlapping jurisdiction. Stephen Collins from Hotmail said that the Home Office had not explained how it would address the possibility of obligations in the draft Bill putting Microsoft in a position of legal conflict with its home state laws in the USA, Ireland and Luxembourg.[166] Emma Ashcroft from Yahoo! was concerned that extending jurisdiction would set a "global precedent" with the United Kingdom being the first State to adopt provisions of this type.[167] She believed that other States would follow, using legislation to limit free expression and infringe privacy rights. She felt that the draft Bill "would create a bewilderingly complex patchwork of overlapping and potentially conflicting laws, and put companies like ours in a very difficult position where we have to make difficult decisions about how to be consistent in our approach to law enforcement and protecting our users." [168]

162 Q 48

163 Q 926

164 Q 930

165 Q 557

166 Q 550

167 Q 554

168 Q 582

240. Colin Crowell from Twitter said that there were questions about the assertion of authority over a company subject to US laws,[169] and referred to the "conundrum" of how to deal with use data that might be related to non-UK citizens and that might be part of a communication with a United Kingdom citizen.[170] Simon Milner told us that Facebook would "strongly oppose" a measure requiring it to violate the law of another State. It would want the Government to frame any notice so as to require the retention of data only in respect of United Kingdom users, since otherwise Facebook might be violating the law in the USA or in EU Member States. Facebook would therefore store data only in respect of United Kingdom users, and might resort to the courts in the event of measures requiring the retention of data relating to other users. But this was not a step Facebook would want to take.[171]

241. We believe that these are significant and valid concerns, and that the Government have not fully considered the jurisdictional issues raised by their proposals or discussed them in detail with the overseas CSPs. It would be wrong to use an United Kingdom statute to seek to impose on the CSPs requirements which conflict with the laws of the countries where they are based, and if this was to happen it would risk jeopardising the good relations which currently exist and on which much depends.

242. **We have heard from the Home Office and some of the overseas CSPs that relations between them are generally good, and that data is routinely provided on request without the need for legislation. The Bill should not jeopardise these good relations.**

243. **The Government has no legal authority to ask overseas providers to generate or retain information for which they have no business purpose. If, following proper consultation with overseas providers, it is thought necessary to have a legal basis for the Government to require overseas providers to retain more data, and a legal basis to allow the Government to help with the costs of doing so, it may be sensible to retain the extra-territorial provisions of the legislation, even if they are of doubtful effectiveness. But this should not be done unless consultation demonstrates that it will not jeopardise cooperation with overseas CSPs.**

Mutual Legal Assistance Treaties (MLAT)

244. Where they are unable to access data in any other way, United Kingdom law enforcement authorities can use the arrangements for international mutual legal assistance which allow the judicial and prosecuting authorities of one State to seek from the authorities of another State help in the prevention, detection and prosecution of crime. The procedure is governed by the Crime (International Co-operation) Act 2003. If it appears to a court on an application made by, for example, the Crown Prosecution Service that an offence has been or may be committed, or is being investigated, the court may request assistance from another State which will then pass the request to own its prosecution or law enforcement authorities.

169 Q 610

170 Q 617

171 Ibid.

245. The procedure is governed by bilateral mutual legal assistance treaties (MLAT). The United Kingdom has MLATs with most other states with which it has good relations. The invariable pattern of these agreements is for each State party to designate a central authority through which all incoming and outgoing requests are channelled. In the United Kingdom the Home Office is the central authority through which requests for communications data held overseas will be sent to the central authority of the State where the communications data is held. That authority will seek the requested information through its own procedures and forward it back to the central authority of the requesting State which will transmit it back to the original requesting authority.

246. There are a number of problems:

- the time involved;
- the fact that the request must be seen to have been initiated by a prosecuting authority such as the CPS, rather than the police;
- the premature involvement of the CPS (who have limited resources) in an investigation or operation that is at a formative stage;
- the detail and amount of information required to satisfy the standards of the various treaties (for example full summary of evidence, witness statements, transcripts of interviews etc).

247. A number of our witnesses criticised the system. Charles Farr explained:

> "MLATs have not been designed, either by us or by the Department of Justice, to facilitate ongoing investigations on a day to day basis. They never have been, and it would be very difficult to turn them into that. ... Neither we nor the Department of Justice can easily see how an MLAT can be transformed into an almost real-time tool for the exchange of data." [172]

248. In the case of child exploitation time is often crucial, and Peter Davies, the Chief Executive of CEOP, was also critical:

> "I think it works slowly. It certainly does not work in operational fast time … It works with those countries with which we have a mutual legal assistance treaty, but not with those with which we do not, and my centre is quite often in the position of having to ask for help in the absence of any such treaty. Generally, we do quite well at getting it, but it is pretty random. I would not see the MLAT process as an alternative to the legislation as proposed." [173]

249. Just as there is nothing to stop the authorities requesting data from CSPs, so there is, as Mr Davies said, nothing to stop them seeking help informally from authorities in other countries, whether or not the United Kingdom has MLATs with them. United Kingdom police forces often seek information in this way from colleagues in other countries with which they have good relations. But the MLAT system has the advantage that the legality

172 Q 931

173 Q 1077

of obtaining the information, and its admissibility in evidence, is not in doubt since it is based on an agreement with the State from which the information is sought.

250. Not surprisingly, a number of overseas CSPs supported the MLAT system as a means of resolving jurisdictional issues. For Yahoo! Emma Ashcroft explained:

> "The mutual legal assistance treaty recognises that jurisdiction has limits. Regardless of what is written in this Bill, the UK jurisdiction has limits somewhere, and the mutual legal assistance treaty structure is designed specifically to address that issue. UK law enforcement uses that framework frequently, and there may be room to improve it, but for us it is a framework that gives us legal clarity and gives some order to this very complex international legal framework under which we have to operate."[174]

251. Sarah Hunter agreed, and said that where Google cannot voluntarily comply with a RIPA request it encourages use of MLAT. But she and Stephen Collins from Microsoft both suggested that the system should be speeded up, and that the Government had a part to play.[175]

252. We understand that the slowness of the system can be particularly frustrating when data is required at the investigatory stage. To some extent the remedy is in the hands of the Government. The Home Office is the United Kingdom central authority; it could speed up internal United Kingdom procedures, and attempt to influence foreign States to do the same. The MLAT system will never be as fast as direct approaches to overseas CSPs but, as our witnesses emphasised, it has the advantage of legal certainty.

253. **It does not require legislation for the United Kingdom, when it is the requesting State, to minimise the bureaucratic delays in this country in the operation of the MLAT process, and to prioritise its own requests. This is something the Home Office, as the United Kingdom central authority, should address forthwith. Given that many of the overseas CSPs are based in the United States, the Government should take advantage of the special relationship with the United States to ensure that bilateral arrangements with them are expedited.**

174 Q 556

175 QQ 558, 563

7 Cost and benefits

Overall cost of the legislation

254. The Impact Assessment published with the draft Bill states: "Total discounted economic costs over the 10 years starting from 2011/12 are estimated to be £1.8 billion. This represents the cost of the programme without allowing for inflation, Value Added Tax and depreciation." The main categories of cost are stated to be:

- **Current work** with major UK telecommunication operators to implement data retention solutions resulting from the EUDRD;
- **Operational enhancements** undertaken within the limits of current legislation with a particular focus on training investigators;
- **Risk reduction** to help identify the technical and operational challenges in implementing a long-term solution; and
- **Strategic work** to develop and implement the preferred option (2)[176] to address the challenge presented by new and emerging technologies, requiring new legislation.

255. No breakdown of the figure of £1.8 billion is given. At their first evidence session Home Office officials were asked for further details,[177] which they supplied in a confidential annex to their written evidence, and further elaborated in later oral evidence.[178]

256. The CSPs will incur costs mainly for retaining, securely storing, accessing and ultimately destroying communications data, but also for matters such as training. The Home Office gave a figure of £859m over 10 years for reimbursing the additional costs to the private sector. This is nearly half of the overall figure of £1.8 billion. However this figure must be highly suspect, because it was calculated with little or no input from the CSPs. Giving evidence in September, Mark Hughes for Vodafone said flatly: "We have never been consulted on cost."[179] Stephen Collins for Microsoft told us: "It is very hard to estimate what the costs will be when we do not know what we would be expected precisely to do under the secondary legislation on the code of practice ... the draft Bill talks about the level of security required. It is almost an absolute that the data must be securely stored—not "reasonably securely" but "securely": 100%. That creates an awful lot more cost as well…."[180] The witnesses for Facebook and Twitter agreed.

257. Nevertheless, in his subsequent evidence Charles Farr told us that, on the basis of the regular discussions the Home Office had with the UK CSPs on their costs in implementing the RIPA arrangements, "we know in quite a high level of detail what those costs comprise [and] we have already formed the basis of our calculations about the costs that the CSPs may incur in future. We have added in considerable optimism bias on top of that. I would

176 i.e. new legislation

177 QQ 73-77

178 QQ 882-910

179 Q 472

180 QQ 653-654

not want you to conclude that we have plucked these figures out of thin air. They are based on existing costs which we have already established with the providers. It is still our view … that these figures accurately represent the likely cost going out to 2020."[181] The business case was being "refreshed", but he did not anticipate that it would come up with a figure higher than £1.8 billion.

258. Mr Farr repeated that this figure "builds in quite a lot of optimism bias". For Microsoft, Mr Collins had told us: "… the costs will increase. Even if we gave you a figure now, I would be willing to bet money that in 10 years' time that cost will have multiplied grotesquely."[182] The figure he was referring to was the cost to CSPs. We think he would be betting on a certainty. Future developments are entirely unpredictable. It is impossible to foresee what new communications providers or forms of communication may emerge, perhaps from overseas, that will suddenly become a significant player and incur recoverable costs. We expect the overall cost to the taxpayer over the next decade to exceed £1.8 billion by a considerable margin.

Covering the costs of CSPs

259. Clause 26 of the draft Bill provides that the Secretary of State must ensure that arrangements are in place to secure that CSPs receive "an appropriate contribution in respect of such of their relevant costs [i.e. the costs of performing activities permitted or required by the Bill] as the Secretary of State considers appropriate". The arrangements put in place may require an audit of any claim for costs. Additionally, the Secretary of State may determine whether or not contributions should be made to particular operators and the appropriate level of contribution (if any) in each case.

260. This replaces a much simpler provision in RIPA for the making of "appropriate contributions" to the costs incurred by CSPs in complying with notices under section 22(4) of RIPA. At present the "appropriate contributions" have been 100%, as Mark Hughes confirmed on behalf of Vodafone: "In my experience, appropriate contributions have always been 100% of our costs. We are covered in this whether we are developing the capability that we have been asked to or whether it is for the operating expenditure, year on year, based on our stores of our disclosures." But, he added, "one of the things that we would like to see in future years … is that 100% being written down and more enshrined in the legislation."[183] This anxiety was shared by all the CSPs, all of which wanted the obligation to give them full cost recovery to be on the face of the Bill.[184]

261. Mr Farr told us that he has sought to allay the concerns of the CSPs: "As you know, under the existing provisions we cover the costs incurred by CSPs in meeting the obligations set out in the legislation. We have said, and told CSPs last week in another meeting, that we would continue that commitment through and beyond this legislation."[185] He added: "The intention is to cover their costs…. We have said right the way along that the principle of this Bill is to have co-operation, consultation, and that must include a

181 Q 883

182 Q 654

183 Q 450

184 See e.g. the written evidence of Everything Everywhere, of ISPA (paragraph 18), and of BT (paragraph 7).

185 Q 850

sensible discussion about costs where they are not immediately apparent." He stipulated that the costs should be "reasonable". Clause 26(4) allows claims for costs to be audited. If, subject to these two provisos, it is the intention of the Government (as we think it should be, if they wish to enjoy the continued cooperation of the CSPs) to reimburse in full the costs they necessarily incur in complying with the legislation, we think this undertaking should be on the face of the Bill.

262. **We are concerned that the Home Office's cost estimates are not robust. They were prepared without consultation with the telecommunications industry on which they largely depend, and they project forward 10 years to a time where the communications landscape may be very different. Given successive governments' poor records of bringing IT projects in on budget, and the general lack of detail about how the powers under the Bill will be used, there is a reasonable fear that this legislation will cost considerably more than the current estimates.**

263. **The Government's commitment to reimburse CSPs the necessary cost to them of complying with the requirements which would be imposed on them by this legislation should appear on the face of the Bill.**

Benefits

264. The Home Office's impact assessment estimates the benefits from the draft Bill in the ten years to 2020/21 at £5.0 to £6.2 billion. With a cost estimate of £1.8 billion, this gives an estimate of net benefits between £3.2 and £4.4 billion. The Home Office explained that this is regarded as "cautious", and: "Only benefits that can be ascribed a monetary value with confidence are considered in the business case. These are revenue loss prevented; assets seized; lives saved; children safeguarded; and paedophile rings disrupted."[186]

265. The monetary value ascribed to revenue loss prevented including tax fraud is £2,008 million, and £627 million is the benefit from facilitating seizure of criminal assets. Donald Toon from HMRC told us that in 2011 the use of communications data was "directly related to about £850 million of protected revenue".[187] We have no means of knowing how accurate these estimates will be, spread over the coming ten years, but we have no reason to doubt that very considerable sums will be saved under these two headings—though whether the sums saved will exceed the cost of the legislation must be a matter for speculation. But we are also asked to accept that a monetary value of £86 million can be ascribed "with confidence" under the heading "children safeguarded or protected from sexual abuse", or £171 million for "high risk child sexual offenders networks disrupted or dismantled". Certainly these would be very valuable achievements, but we fail to understand how they can be ascribed a detailed monetary value in this context.

266. This is demonstrated most clearly in the figures we are asked to accept for "saving and safeguarding lives: £2,084–£3,334 millions". These figures are reached as follows. On the advice of the police and others involved it is assumed that lives are saved in between 25% and 40% of threat to life cases. This would give an estimate of 1,265 to 2,020 lives saved over the next ten years. Each life is given a value of £1,792,398—a figure derived from a

186 Paragraph 105

187 Q 128

Home Office publication which places a financial value on crime, including homicide, taking account of factors such as the cost to the criminal justice system and the cost of lost output.[188] Mr Farr described it as "a Treasury figure used in a number of different scenarios across government."[189]

267. It may be that, for some purposes, it is useful to be able to ascribe a monetary value to a life saved. We fail to understand what relevance this can have in the impact assessment for a draft Bill. The figures are used to attempt to show that the taxpayer, by spending £1.8 billion over ten years, will recoup perhaps three times that amount, when this is not the case. To suggest that these estimates can be used to calculate a net benefit from enactment of the draft Bill at between £3.2 and £4.4 billion is simply fanciful and misleading.

268. The use of figures in this way points to a further absurdity. We are asked to believe that access to a further 10% of communications data over and above the 75% already available would save perhaps a further 150 lives a year. Logically, it should follow that the communications data currently available is saving around 1,000 lives a year, but the Home Secretary told us that the figure was "1,000 to 2,000 lives being saved" over the 10 year period. None of our witnesses could provide specific evidence of significant numbers of lives saved to date.[190]

269. **The figure for estimated benefits is even less reliable than that for costs, and the estimated net benefit figure is fanciful and misleading. It ought not to be used to influence Parliament in deciding on the relative advantages and disadvantages of this legislation. Whatever the benefits of the Bill, they are unlikely to be financial.**

270. **A new cost benefit analysis should be presented alongside any redrafted Bill. It should be based on the wider consultation and narrower powers; it should contain significantly more detail than the current impact assessment; it should separate monetary benefits from other unquantifiable benefits such as potential lives saved; and it should refer to past evidence.**

The disadvantages to United Kingdom business

271. There are disadvantages to business other than the purely financial, and the London Internet Exchange (LINX) made a number of points which are troubling some of the CSPs.[191] They said, and we agree, that:

> "All the UK's best and brightest prospects for economic growth depend on access to the best and most innovative Internet services. The Internet sector therefore has an enormous wealth multiplier factor, especially for a high-value high-skill internationally trading economy like ours. Accordingly, any action that undermines

188 "The economic and social cost of crime against individuals and households 2004/04", Economics and Resource Analysis Research, Development and Statistics Directorate, Home Office.

189 Q 898, HM Treasury Green Book: Appraisal and Evaluation in Central Government. Annex 2, paragraphs 26-33, deals with the value of a prevented fatality or prevented injury. The measurement is based on an individual's willingness to pay for a reduction in the risk of death (or their willingness to accept a new hazard and the ensuing increased risk), from which the value of a prevented fatality can be inferred.

190 QQ 904-907

191 Written evidence, paragraphs 49-56.

> the positive effect of the Internet sector could have serious economic consequences, with implications well beyond the companies directly affected themselves."

272. While LINX welcome the Government's commitment to reimburse financial costs directly attributable to the legislation, they point out that there are other costs which will inevitably be unrecoverable. Costs of hardware for the construction of substantial new systems, data storage facilities, and access, search and retrieval mechanisms, would be recoverable, but what of the incalculable, and hence irrecoverable, opportunity cost, as senior executives and the most talented technical staff are diverted into delivering these requirements and away from commercial goals? Other costs which are not direct financial costs might include performance degradations, reductions in network and service resilience, or the inability to offer a particular service to customers when other, foreign, operators were not so constrained. Such costs would not be recoverable as direct financial costs under the draft Bill, and they would make the telecommunications operator that incurred them less attractive to its customers and users.

273. LINX's conclusion is that UK-based operators will find themselves at a competitive disadvantage. Foreign operators would have a significant incentive to avoid exposing themselves to the possibility of incurring such irrecoverable costs, by avoiding establishing themselves in the United Kingdom. They might also make it more likely that communications service providers based outside the United Kingdom will prevent their service from being accessed from within the United Kingdom.

274. The Internet Service Providers' Association, made a similar point:

> "The Draft Bill has the potential to put the UK at a competitive disadvantage and destabilise the market, with the UK seen as a less attractive and more onerous place to do business digitally, affecting both inward investment and services being made available. In challenging economic times we question whether this should be a government priority."

We sympathise with these views.

275. **We believe that the Government, in imposing obligations on CSPs, should bear in mind the importance of preserving their competitiveness, and minimising damage to the reputation of the United Kingdom as an attractive base for conducting business.**

276. The Government should also pay particular attention to the problems of any smaller companies it may think of targeting. We heard evidence from Trefor Davies, the Chief Technology Officer of Timico Ltd. As he told us, they are not a small company; they have about £40 million turnover, and a couple of hundred staff of whom maybe 40 are engineers, but the real core of the team who would have to work on compliance with new legislation is only six people: network engineers, systems engineers, and applications engineers. "The biggest problem we would have as a business is the amount of effort that we would have to put in, in the first place, to setting [the filter] up ... Smaller ISPs may only have six or 10 engineers to do what we do with 40 or 50 engineers, but it would still take the same amount of effort, so the smaller the ISP the more disruption and harm it makes."[192]

192 Q 972

277. **Before imposing any obligations on smaller CSPs, the Government should consider whether these are strictly necessary, bearing in mind the real burden this may impose on resources. They should discuss with the company how they can best cooperate to cause the least disruption to the business.**

8 Conclusion, and summary of recommendations.

Overall conclusion

278. It is the duty of government—any government—to maintain the safety and security of law-abiding citizens, so that they may go about their lives and their business as far as possible in freedom from fear. This is not only in the public interest; it is in the interest of law-abiding members of the public. For this the law enforcement authorities should be given the tools they need. Reasonable access to some communications data is undoubtedly one of those tools.

279. Government also has a duty to respect the right of law-abiding citizens to privacy and their ability to go about their lawful activities, including their communications, without avoidable intrusions on their privacy.

280. These duties have the potential to conflict. The law enforcement agencies, including for this purpose the Home Office, tend not unnaturally to give greater weight to the requirements of safety and security. Most of the other people and organisations who have given evidence to us have formally recognised, sometimes with little more than a perfunctory nod, the need for the law enforcement agencies to have limited access to at least some communications data, but have placed greater weight on the need to respect privacy. Where and how the balance should be struck between these conflicting duties in a mature Parliamentary democracy Parliament has to decide; indeed perhaps only Parliament can in the end decide. It has been our purpose in scrutinising this draft Bill to help Parliament in the challenging task of reaching its decisions when it comes to deal with proposals for legislation dealing with these matters.

281. Our overall conclusion is that there is a case for legislation which will provide the law enforcement authorities with some further access to communications data, but that the current draft Bill is too sweeping, and goes further than it need or should. We believe that, with the benefit of fuller consultation with CSPs than has so far taken place, the Government will be able to devise a more proportionate measure than the present draft Bill, which would achieve most of what they really need, would encroach less upon privacy, would be more acceptable to the CSPs, and would cost the taxpayer less. We make detailed recommendations accordingly on the content of a revised Bill.

Summary of recommendations for the way forward

Is there a need to access more communications data?

282. Part of the data gap is down to a lack of ability on behalf of law enforcement agencies to make effective use of the data that is available. Addressing this should be a priority. It does not require fresh legislation but will involve additional expenditure.

283. We accept that IP addresses and web logs and data generated for business purposes but not retained by overseas CSPs are three data types which the law enforcement and other agencies cannot always access. We discuss in this report whether access to these data

categories is necessary and if it is to be enabled, the additional safeguards which will need to be introduced.

Failure to consult

284. Before re-drafted legislation is introduced there should be a new round of consultation with technical experts, industry, law enforcement bodies, public authorities and civil liberties groups. This consultation should be on the basis of the narrower, more clearly defined set of proposals on definitions, narrower clause 1 powers and stronger safeguards which are recommended in this report. The United Kingdom and overseas CSPs should be given a clear understanding of the exact nature of the gap which the draft Bill aims to address so that those companies can be clear about why the legislation is necessary.

285. Even though many of them are prepared to cooperate on a voluntary basis, they should also be told what obligations might be imposed on them. For many, their willingness to cooperate voluntarily will be reinforced if there is a statutory basis for the requirement.

286. Meaningful consultation can take place only once there is clarity as to the real aims of the Home Office, and clarity as to the expected use of the powers under the Bill. CSPs should be consulted on the basis of drafts of the specific notices which will be served on them; these will have the detail of the obligations to be imposed on them, and enable them to undertake a better assessment of feasibility and of the resources and timescales involved.

The breadth of clause 1

287. The Home Office was able to tell us of specific types of data that are currently not routinely retained for business purposes by United Kingdom (and many overseas) CSPs and which would be useful to law enforcement and other investigations. It is the Home Office's intention to issue notices under the Bill to ensure that an unknown number of CSPs retain these specific types of data. The Home Office has however made clear that it does not currently need the power under this legislation to require other types of data be retained, and does not for the present intend to issue notices going more widely (except to CSPs which are not covered by the EU Data Retention Directive, which might be asked under this legislation to retain for 12 months data which they already create for business purposes). Clause 1 therefore should be re-drafted with a much narrower scope, so that the Secretary of State may make orders subject to Parliamentary approval enabling her to issue notices only to address specific data gaps as need arises.

288. The Home Office has argued that there is a case for keeping clause 1 wide because there may be other data types that emerge from time to time which will be important to law enforcement but will not be routinely retained by CSPs for business purposes. We do not accept that this is a good reason to grant the Secretary of State such wide powers now. We do not think that Parliament should grant powers that are required only on the precautionary principle. There should be a current and pressing need for them.

289. We do however accept that, depending on how the communications world develops, the Home Office may in future need the power to require the retention of other data types. Parliament and government both need to accept that legislation that covers the internet

and other modern technologies may need revisiting and updating regularly. We have considered how the Secretary of State might be given powers in the future to allow her to address new and significant data gaps if and when they emerge. The alternatives seem to be either primary legislation on each occasion, or a power to amend clause 1 by order subject to a super-affirmative procedure which would guarantee fuller Parliamentary consideration than a standard affirmative order.

290. We attach in Appendix 7 a consideration of the relative advantages and disadvantages of each course. On balance our preference is for an order subject to the super-affirmative procedure. We recognise that this will impose obligations on Parliament which it will have a duty to discharge effectively.

291. We recommend that a narrower clause 1 should allow notices to be served on CSPs requiring them to generate and retain subscriber data relating to IP addresses.

292. Whether clause 1 should allow notices that require CSPs to retain web logs up to the first "/" is a key issue. The Bill should be so drafted as to enable Parliament to address and determine this fundamental question which is at the heart of this legislation.

293. The Home Office and law enforcement agencies and (so far as we know) the intelligence and security services think that access to web logs is essential for a wide range of investigations. The civil liberties organisations argue that web logs are potentially a highly intrusive form of communications data and that generating and storing web logs gives rise to unacceptable risks to the privacy of individuals.

294. We are confident that the safeguards in the draft Bill, together with the recommendations we make to strengthen those safeguards, can provide a high degree of protection against abuse of communications data or inadvertent error by public authorities. We acknowledge that storing web log data, however securely, carries the possible risk that it may be hacked into or may fall accidentally into the wrong hands, and that, if this were to happen, potentially damaging inferences about people's interests or activities could be drawn. Parliament will have to decide where the balance between these opposing considerations should be struck.

295. In 2003, Parliament considered the Code of Practice for the Acquisition and Disclosure of Communications Data which included the guidance that web addresses up to the first "/" should be considered to be communications data. The presentation of this Bill provides an opportunity for Parliament to review this controversial issue.

296. We also recommend that the Home Office should examine whether it would be technically and operationally feasible, and cost effective, to require CSPs to keep web logs only on certain types of web services where those services enable communications between individuals.

297. The Home Office knows that not all overseas CSPs will comply with retention notices. It is for this reason that the notices issued under clause 1 may require United Kingdom CSPs to keep third party data traversing their networks. United Kingdom CSPs are rightly very nervous about these provisions. The Home Office has given an oral commitment to United Kingdom CSPs that the Home Secretary will invoke the third party provisions only after the original data holder has been approached and all other avenues have been

exhausted. The Home Office has also given a commitment that no CSP will be asked to store or decrypt encrypted third party data. These commitments should be given statutory force.

The Request Filter

298. Whoever operates the Request Filter will need significant expertise and staff at their disposal. If CSPs update their systems and the Request Filter is not adjusted there is a risk that results will be incomplete, rendering them useless. The Bill should be amended to say that the Secretary of State may transfer her responsibilities for operating the Request Filter to the soon to be established National Crime Agency but not to other bodies. The National Crime Agency will need appropriate resources and this should be reflected in the revised cost/benefit analysis.

299. The Request Filter will speed up complex inquiries and will minimise collateral intrusion. These are important benefits. On the other hand the Request Filter introduces new risks, most obviously the temptation to go on "fishing expeditions". New safeguards should be introduced to minimise these risks. In particular the IoCC should be asked to investigate and report on possible fishing expeditions and to test rigorously the necessity and proportionality of Filter requests.

Who should be able to access communications data?

300. Any public authorities which make a convincing business case for having access to communications data should, like the six we have specified in paragraph 25, be listed on the face of the Bill. We expect this to be a greatly reduced number when compared to the authorities currently listed in the Regulation of Investigatory Powers (Communications Data) Order 2010.

301. Any necessary changes to this list should be made by order subject to the super-affirmative procedure which includes the opportunity of scrutiny by the appropriate Select Committee.

For what purposes should communications data be used?

302. Of the ten permitted purposes in clause 9(6) of the draft Bill, seven were in RIPA originally, two were added by order in 2006, and one is new. We think it unlikely that there are any other as yet unidentified purposes which could properly be added. The House of Lords Delegated Powers and Regulatory Reform Committee recommended that any additions to this list should require primary legislation. We agree. Clause 9(7), which allows the Secretary of State to add further permitted purposes by order, should be deleted.

303. We are concerned that the long list of permitted purposes for which communications data can be requested adds to public disquiet about the breadth of the Bill. While we do not make specific recommendations about how this list could be shortened, we recommend that the Government should consult on whether all the permitted purposes are really necessary.

Definitions of communications data

304. The language of RIPA is out of date and should not be used as the basis of new legislation. The Bill should be re-drafted with new definitions of communications data. The challenge will lie in creating definitions that will stand the test of time. There should be an urgent consultation with industry on changing the definitions and making them relevant to the year 2012.

305. The definitions of use, subscriber and traffic data are particularly problematic. Subscriber data should not be a catch-all for data that does not meet the other definitions. Currently the definition of subscriber data could be read to cover all sorts of data that social networks and other services keep on their customers which can be highly personal and is not traditionally thought of as communications data. A new definition of subscriber data is needed that simply covers the basic subscriber checks that are the most commonly used. How to define subscriber data should be a key element of the consultation, but the evidence we have received leads us to suggest that the definition should include checks on the name, date of birth, addresses and other contact information held on the subscriber to a communication service; for each service the customer's unique ID (e.g. mobile number, e-mail address or username); the activation, suspension and termination dates of an account and payment and billing information.

306. A new hierarchy of data types needs to be developed. Data should be divided into categories that reflect how intrusive each type of data is. The following principles could be useful to determine and measure the degree of privacy intrusion of communications data: public attitudes about the extent to which a certain type of communications data is private; the risk of identifying details of an individual's life, behaviour, beliefs, that they would reasonably consider personal; the risk of data being misused (i.e. used in a way not set out by the legislation) or accessed by third parties, either intentionally or not.

307. It is imperative that everything is done to make clear that content cannot be requested under the provisions of this legislation. Content is not defined in the draft Bill. Although it may not be possible to define content clearly beyond the fact that it is the "what" of a communication, it is nevertheless important that the content should be expressly excluded from all categories of communications data.

The authorisation process

308. The SPoC process should be enshrined in primary legislation. A specialist centralised SPoC service should be established modelled on the National Anti-Fraud Network service which currently offers SPoC expertise to local authorities. The Home Office should consider allowing police forces to bid to run this service. This new service should be established by statute, and all local authorities and other infrequent users of communications data should be required to obtain advice from this service.

309. Although approval by magistrates of local authority authorisations is a very recent change in the law, we think that if our recommendations are implemented it will be unnecessary to continue with different arrangements applying only to local authorities.

The Interception of Communications Commissioner

310. The IoCC should carry out a full review of each of the large users of communications data every year. While sampling is acceptable as a way of dealing with large users, the requests of users making fewer than 100 applications in a year should be checked individually. The annual report of the IoCC should include more detail, including statistics, about the performance of each public authority and the criteria against which judgements are made about performance. It should analyse how many communications data requests are made for each permitted purpose. For this the IoCC will need substantial additional resources, both as to numbers and as to technical expertise. There should be full consultation with him on this. His role should be given more publicity.

311. The IoCC's brief should explicitly cover the need to provide advice and guidance on proportionality and necessity, and there should be rigorous testing of, and reporting on, the proportionality and necessity of requests made.

312. The IoCC will be key to public confidence in the Request Filter. The IoCC will need the necessary expertise properly to examine the operation of the Request Filter. He will have to report on the scale of searches via the Request Filter and rigorously test the necessity and proportionality of requests put to the Filter. All this information should be included in the public section of his annual report so that if there are any signs that the Filter is resulting in more intrusive requests Parliament can review the legislation.

The Information Commissioner

313. Clause 22(5) should be reviewed. If the Government believe that additional safeguards can be provided by the Information Commissioner, they should undertake detailed discussions with him as to what such safeguards might be, how they might be undertaken, and what additional powers and resources he might need. The Bill should make clear that the Information Commissioner will need to be shown all notices issued under clause 1.

Other Surveillance Commissioners

314. Work should be done to rationalise the number of commissioners with responsibility for different areas of surveillance. This work should aim to simplify the situation and make it easier for the public to understand, while ensuring that all surveillance powers are subject to rigorous oversight. Consideration should be given to a new unified Surveillance Commission reporting to parliament with multi-skilled investigators and human rights and computer experts.

Security and destruction of data

315. We consider the Home Office's cost estimates may underestimate the cost of security and destruction of data. Since the cost of security and destruction will ultimately be borne by the taxpayer, the Home Office will have to carry out a careful cost/benefit analysis and obtain advice and assurances from a wider body of experts that the companies that stand to earn money from devising secure storage solutions.

Offence of misuse of communications data by a public authority

316. The House of Commons Justice Committee recommended that the power under section 77 of the Criminal Justice and Immigration Act 2008 should be exercised "without further delay". Nearly a year later the Home Affairs Committee reached the same conclusion. We agree with the Information Commissioner and with both these Committees that this power to allow custodial sentences to be imposed in appropriate cases should be exercised without delay.

317. The Bill should provide for wilful or reckless misuse of communications data to be a specific offence punishable in appropriate cases by imprisonment.

Jurisdictional issues

318. We have heard from the Home Office and some of the overseas CSPs that relations between them are generally good, and that data is routinely provided on request without the need for legislation. The Bill should not jeopardise these good relations.

319. The Government has no legal authority to require overseas providers to generate or retain information for which they have no business purpose. If, following proper consultation with overseas providers, it is thought necessary to have a legal basis for the Government to ask overseas providers to retain more data, and a legal basis to allow the Government to help with the costs of doing so, it may be sensible to retain the extra-territorial provisions of the legislation, even if they are of doubtful effectiveness. But this should not be done unless consultation demonstrates that it will not jeopardise cooperation with overseas CSPs.

320. It does not require legislation for the United Kingdom, when it is the requesting State, to minimise the bureaucratic delays in this country in the operation of the MLAT process, and to prioritise its own requests. This is something the Home Office, as the United Kingdom central authority, should address forthwith. Given that many of the overseas CSPs are based in the United States, the Government should take advantage of the special relationship with United States to ensure that bilateral arrangements with them are expedited.

Costs and benefits

321. We are concerned that the Home Office's cost estimates are not robust. They were prepared without consultation with the telecommunications industry on which they largely depend, and they project forward 10 years to a time where the communications landscape may be very different. Given successive governments' poor records of bringing IT projects in on budget, and the general lack of detail about how the powers under the Bill will be used, there is a reasonable fear that this legislation will cost considerably more than the current estimates.

322. The Government's commitment to reimburse CSPs the necessary cost to them of complying with the requirements which would be imposed on them by this legislation should appear on the face of the Bill.

323. The figure for estimated benefits is even less reliable than that for costs, and the estimated net benefit figure is fanciful and misleading. It ought not to be used to influence

Parliament in deciding on the relative advantages and disadvantages of this legislation. Whatever the benefits of the Bill, they are unlikely to be financial.

324. A new cost benefit analysis should be presented alongside any redrafted Bill. It should be based on the wider consultation and narrower powers. It should contain significantly more detail than the current impact assessment and should separate monetary benefits from other unquantifiable benefits such as potential lives saved and refer to past evidence.

325. We believe that the Government, in imposing obligations on CSPs, should bear in mind the importance of preserving their competitiveness, and minimising damage to the reputation of the United Kingdom as an attractive base for conducting business.

326. Before imposing any obligations on smaller CSPs, the Government should consider whether these are strictly necessary, bearing in mind the real burden this may impose on resources. They should discuss with the company how they can best cooperate to cause the least disruption to the business.

Appendix 1: Members and interests

The Members of the Joint Committee that conducted this inquiry were:

Lord Armstrong of Ilminster
Rt Hon Lord Blencathra (Chair)
Baroness Cohen of Pimlico
Lord Faulks
Rt Hon Lord Jones
Lord Strasburger
Rt Hon Nicholas Brown MP
Michael Ellis MP
Dr Julian Huppert MP
Stephen Mosley MP
Craig Whittaker MP
David Wright MP

Declaration of Interests

The following interests have been declared:

Lord Blencathra: Former Minister of State at the Home Office.

Lord Armstrong of Ilminster: Former Permanent Secretary of the Home Office and Secretary of the Cabinet.

Dr Julian Huppert MP: Member of the Advisory Council of the Open Rights Group.

Mr Stephen Mosley MP: A shareholder in a small IT services company.

Full lists of Members' interests are recorded in the Commons Register of Members' Interests:

http://www.publications.parliament.uk/pa/cm/cmregmem/contents.htm

and the Lords Register of Interests:

http://www.parliament.uk/mps-lords-and-offices/standards-and-interests/register-of-lords-interests/

Appendix 2: Witnesses

Tuesday 10 July 2012

QQ 1-96

Richard Alcock, Director of Communications Capability Directorate, Home Office, **Charles Farr,** Director General, Office of Security and Counter-Terrorism, Home Office and **Peter Hill,** Head of Unit for Pursue Policy and Strategy Unit, Home Office

Wednesday 11 July 2012

QQ 97-126

Mr David Davis MP, Member of Parliament, **Nick Pickles**, Director, Big Brother Watch, **Jim Killock**, Executive Director, Open Rights Group, and **Gus Hosein**, Executive Director, Privacy International

Thursday 12 July 2012

QQ 127-220

Donald Toon, Director of Criminal Investigation, HMRC, **Cressida Dick**, Assistant Commissioner, MPS, **Gary Beautridge**, CC/Assistant Chief Constable, ACPO, **Trevor Pearce**, Director General, SOCA, and **Peter Davies**, Chief Executive Officer, CEOP; **Daniel Thornton**, Head of Enforcement (-Legal-), FSA, **Councillor Paul Bettison**, Leader of Bracknell Forest Council, LGA Regulatory Champion and Member of the LGA Safer Communities Board, **Gillian McGregor**, Director of Operational Intelligence, UKBA, and **Nick Tofiluk**, Director of Regulatory Operations, Gambling Commission.

Tuesday 17 July 2012

QQ 221-329

Nick Pickles, Director, Big Brother Watch, **Jim Killock**, Executive Director, Open Rights Group, **Rachel Robinson**, Policy Officer, Liberty, and **Angela Patrick**, Director of Human Rights Policy, Justice; **Professor Anthony Glees**, Director, Centre for Security and Intelligence Studies, University of Buckingham, and **Dr Julian Richards**, Co-Director, Centre for Security and Intelligence Studies, University of Buckingham

Tuesday 4 September 2012 — QQ 330-416

Professor Ross Anderson, Professor of Security Engineering, Computer Laboratory, University of Cambridge, **Professor Sadie Creese**, Professor of Cybersecurity, Department of Computer Science, University of Oxford, **Professor Peter Sommer**, Visiting Professor, De Montfort University Cyber Security Centre, and **Glyn Wintle**, Chief Consultant, Firewolf

Wednesday 5 September 2012 — QQ 417-546

Jonathan Grayling, Head of Law Enforcement Liaison, Everything Everywhere, **Bob Hughes**, Government Programme Manager, Telefónica UK – O2, **Mark Hughes**, Managing Director Security, BT, **Mark Hughes**, Head of Corporate Security, Vodafone, and **Simon McCready**, Group Risk Director, Virgin; **Nicholas Lansman**, Secretary General, Internet Services Providers' Association (ISPA), **Malcolm Hutty**, Head of Public Affairs, London Internet Exchange (LINX), and **Jimmy Wales**, appearing in a personal capacity

Thursday 6 September 2012 — QQ 547-659

Sarah Hunter, Head of UK Public Policy, Google; **Stephen Collins,** Head of EU Policy, Microsoft, for Hotmail; and **Emma Ascroft**, Director of Public Policy, Yahoo!; **Simon Milner**, Director of Policy for UK & Ireland, Facebook**; Colin Crowell**, Head of Global Public Policy, Twitter; **Stephen Collins**, Head of EU Policy, ex-Skype/Microsoft**; Steven Murdoch**, Chief Research Officer, the Tor Project, and Senior Researcher, University of Cambridge

Tuesday 16 October 2012 — QQ 660-713

Sir Paul Kennedy, Interception of Communications Commissioner, Interception of Communications Commission, and **Joanna Cavan**, Chief Inspector, Interception of Communications Commission; **Christopher Graham**, Information Commissioner

Wednesday 17 October 2012

QQ 714-749

Jamie Bartlett, Demos; **Lord Carlile of Berriew**, former Independent Reviewer of Terrorism Legislation

Tuesday 23 October 2012

QQ 750-839

Henry Porter, Columnist for *The Observer*, **Duncan Campbell**, IPTV, and **Paul Heritage-Redpath**, Product Manager and Solicitor, Entanet Opinion; **Keir Starmer QC**, Director of Public Prosecutions

Wednesday 24 October 2012

QQ 840-933

Richard Alcock, Director of Communications Capability Directorate, **Charles Farr**, Director General, Office of Security and Counter-Terrorism, and **Peter Hill**, Head of Pursue Policy and Strategy Unit, Home Office.

QQ 934-1012

Martin Sutherland, Managing Director, BAE Systems Detica, and **John Davies**, Chief Technology Officer, Global Communications Systems, BAE Systems Detica (Evidence taken in private and not published)

Tuesday 30 October 2012

QQ 1013-1140

Trefor Davies, Chief Technology Officer, Timico Ltd, **David Walker**, Managing Director, Labelled Security Ltd, **Caspar Bowden**, Independent Privacy Advocate, and **Dr Gus Hosein**, Executive Director, Privacy International; **Steve Higgins**, Detective Superintendent, National Policing Improvement Agency, **Sir Peter Fahy**, Chief Constable of Greater Manchester Police, **Peter Davies**, Chief Executive, CEOP, **Alan Lyon**, Detective Superintendent, Greater Manchester Police, and **David Stevenson**, Detective Sergeant, Accredited SPOC Manager, PSNI

Wednesday 31 October 2012

QQ 1141-1207

Rt Hon Theresa May MP, Secretary of State for the Home Department

Appendix 3: Call for written evidence

The Joint Committee on the draft Communications Data Bill, chaired by Lord Blencathra, is conducting pre-legislative scrutiny into the draft Bill and the policies it seeks to implement. The Joint Committee comprises 6 MPs and 6 Peers. It will take oral and written evidence and make recommendations in a report to both Houses. The Joint Committee invites interested organisations and individuals to submit written evidence as part of the inquiry.

Below are specific questions about the details of the draft Bill. The Joint Committee would appreciate written submissions on any of these questions on which you have evidence to contribute. It is not necessary to address every question. The Joint Committee will also welcome other comments related to the draft Bill, even if not directly addressing the questions below.

General:

1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?

2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?

4. What lessons can be learnt from the approach of other countries to the collection of communications data?

5. Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?

6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?

7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?

8. Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base. What might be the effect on business?

Costs:

9. Is the estimated cost of £1.8bn over 10 years realistic?

10. The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5-6bn. Is this figure realistic?

Scope:

11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?

12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by order?

13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?

Use of Communications Data:

14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?

15. Is the proposed 12 month period for the retention of data too long or too short?

Safeguards:

16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?

17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?

18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?

Parliamentary Oversight:

19. Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory?

Enforcement:

20. Are the penalties appropriate for those communications service providers who fail to comply with the requirements of the draft Bill?

21. Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?

Technical:

22. Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?

23. How safely can communications data be stored?

24. Are the proposals for the filtering arrangements clear, appropriate and technically feasible?

25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill ?

26. Are there concerns about the consequences of decryption?

You need not address all these questions.

Appendix 4: Note of visit to Metropolitan Police

Note of visit to Metropolitan Police, 18 October 2012

1. On 18 October 2012 we visited the Metropolitan Police Communications Intelligence Unit (CIU) and met Assistant Commissioner Cressida Dick, Superintendent Paul Jervis, Superintendent Neil Hibberd, Chief Inspector Kenny McDonald, Detective Inspector Steve Carter, Inspector Anthony O'Sullivan, and Roger Smart, barrister. The purpose was to see the Single Point of Contact (SPoC) unit processing applications for authorising access to communications data.

Case Studies

2. We were shown a number of case studies. The first was of a robbery where a man was targeting women in a linked series of robberies in a small area. The suspect would normally steal mobile phones. A breakthrough came when he took a photograph with one of the stolen mobile phones and, because of the setting the owner had on her phone, the photo was automatically uploaded to her internet account. Through this the police were able to make a communications data request which enabled them to narrow down his location. Further evidence was obtained using cell site technology on a phone number obtained by a witness to one of the robberies. This evidence was vital to identify and track the man's activity and link him to six other robberies which he had originally denied being involved in. This case involved multiple separate applications for different types of communications data and that each application had to be justified on the basis of proportionality and necessity and had to be authorised by a senior officer not involved in the case.

3. It was explained that communications data is used sparingly, because it is costly and resource intensive, and because of the need specifically to justify each application and consider the impact of collateral intrusion on innocent people. However in some types of crime, such as suicide, missing children and missing persons it was likely to be the first port of call.

4. The second case study was of a television producer whose website was being bombarded with anti-Semitic abuse. The police suspected that the abuse all stemmed from the same person, who would change their online identifier each time they were blocked. This case could not be pursued because the overseas provider which held the necessary communications data refused to supply it to UK law enforcement. There was an increasing problem of harassment through social media which could not be investigated because overseas CSPs could not or would not provide the necessary communications data. All communications data resulting in a charge would end up in court; the police were increasingly finding that courts were expecting to be presented with this data.

5. Where data rules someone out of an inquiry, it is kept as it is disclosable information in a court case at a later date. Its retention is usually reviewed every 7 years. Under the national data retention scheme implemented following the Soham murders communications data could be retained for 6 years.

6. A further case study was of a recent violent attack on an individual where an iphone was dropped at the scene. This enabled police officers to track 15 suspects from 5am-5pm during a fast moving investigation as they travelled from London to the Midlands. The gang realised what was happening, and started to switch sim cards but could still be tracked because their handsets had been identified. Without this ability they would not have been in a position to make an arrest. Another example was of a gang member gunned down in their car. The police were able to use CCTV, witness evidence, forensic evidence, telephone data and house to house enquiries linked together. They were looking at a rival gang, but using other evidence they were able to identify individual suspects rather than requesting communications data on the entire gang.

7. It was emphasised that no one in the investigating team authorises an application for communications data. An application is sent to someone outside the team to be checked, then submitted for authorisation. In this case, there were two people suspected of being involved. Data was obtained and used to rule them out as it showed they were elsewhere. Subsequently data was obtained on five of the rival gang members. This showed them making contact, coming together and going away again. It linked up with CCTV evidence that showed the car to prove they were there. The data formed part of the wider investigation. There were approximately 500 applications made for different types of data on five people. Suspects often swapped sims but not handsets. Sim swapping led to a large number of applications so that the call data could be attributed to the suspect. To find one sim card it was necessary to apply to each network. If the card was then ditched in two hours, fresh applications to each network would need to be made. Location data only showed that the sim was in that area, so attribution was vital. The data was provided through disclosure in any subsequent court case and could be used to confirm or refute a defence, especially if it relied on the suspect's location at the time.

8. Data was useful both for the investigation and as evidence in a trial. In a kidnapping case the data would be a central line of inquiry in recovering the missing person, and would then be analysed to identify what could be converted into evidence.

9. We saw a demonstration of an app on an iPad that allowed direct communication with another person, while the only information shown would be that the internet was accessed via GPRS. The application listed countries where there were available servers and allowed a choice to be made, for example, of a server in the Czech Republic to have a conversation with someone in the UK.

10. In response to a question on public concerns about access and safeguards, we were told that the independent authorising officers saw their role as akin to that of a magistrate. They would not want to be the authorising officer who got it wrong and caused a case to collapse. The authorising officer often did not know the person making the application. They were liable to internal examination and external audit. They were also likely to be called to court to justify the access authorisation. The training programme dealt with both defence and prosecution use of communications data and with the inspection of the authorisation system.

Communications Intelligence Unit offices

11. We split into small groups to watch individual SPoC officers at work. Different groups saw different applications. These included:

- an example where an overseas CSP operating an international dating website was closed over a weekend and as result a rape investigation was hampered;
- an example where a SPoC turned down a communications data request for call logs in the case of a domestic abuse. The SPoC was concerned that a subscriber check had not been run to confirm that the call logs related to the right suspects, the collateral intrusion of accessing call logs had not been properly assessed and the necessity of the request had not been proved. This SPoC thought he probably referred requests back about 5% of the time.
- an urgent oral request where a written form was not available but where the request had been authorised by a superintendent working on the ground. A verbal case had been made as to necessity and proportionality and a subscriber check had been authorised.
- an example of a request for communications data around delivery of a firearm. The authorisation form was demonstrated, with details of the information required and the process the SPoC would go through to check if the request was justified.
- an example of a computer misuse investigation where a check was being run of the IP address used. The officer explained that often providers used dynamic IPs, some of which were not resolvable. Some could be resolved if ISPs were willing. She explained that she would always advise investigating officers to use such data with caution, as, for example, someone could be using an unsecured wifi access and the owner of the internet connection could be unaware of this.

Evidential value of Communications Data

12. We received a presentation on making use of communications data in evidence from a barrister who had acted both for the prosecution and for the defence in murder, kidnap, paedophile and corruption cases where communications data evidence had been important.

13. In the case of kidnaps, hostages were usually disoriented and did not know where they were or how much time had elapsed. Use of mobiles and cell site analysis gave a narrative of the part played by the different participants. Usually this supplemented other evidence, but there were cases where no prosecution could have been brought without communications data evidence. An example was a case where a kidnapper used both a 'clean' and a 'dirty' phone; however the 'clean' phone revealed where he was, and this connected him to the 'dirty' phone, thus showing that he had been at the kidnap.

14. Communications data was very important for the prosecution of serious fraud. We had been told that criminals would move towards further encryption of their data, but this was not happening in practice. There were examples of supposedly sophisticated individuals who had already been prosecuted using communications data evidence, but still continued

to use mobiles. In one case the FSA had used Blackberry data to prove the purchase of shares; in another a message from the head of a kidnap team to a supposed friend had been used in evidence (though this was not communications data evidence).

15. In cases of attempting to pervert the course of justice, communications data had been used to prove the presence of the person threatening witnesses. Where the pressure on witnesses was successful and the witness declined to testify, an application could be made under s.116 of the Criminal Justice Act 2003 for a statement to be admitted in evidence.

16. The prosecution was under a duty to share all evidence with the defence, including communications data evidence. It could be used as much in support of a defendant's case as in support of the prosecution. Where there were concerns about the credibility of a witness, communications data might be used to support or undermine the witness's testimony. In the course of a trial the judge might ask for additional information from communications data sources, usually to help the defence case.

17. Mutual Legal Assistance Treaties (MLAT) could be used as an alternative route to seek evidence from abroad, but this depended on relations with the particular country. Some were helpful in theory but not in practice. There were also issues of delay and cost.

18. It was very difficult to measure the volume of data which enforcement agencies were unable to access, but there was no doubt that it increased as one moved from telephony to the internet, and further still when one moved to foreign internet. Officers knew very well what data they could access and what they could not access. When mobiles were first used it was feared that they would frustrate reliance on communications data from landlines. On the contrary, they had proved highly beneficial.

Appendix 5: Note of visit to Everything Everywhere

Visit to Everything Everywhere, 25 October 2012

1. The Committee visited the offices of Everything Everywhere (EE) in Hatfield to hear from one of the major communications service providers (CSPs) how they currently dealt with requests for information under the existing legislation, and how they anticipated the draft Bill might affect them if enacted in its current form.

2. The Committee met James Blendis (Vice President, Legal), Jonathan Grayling (Head of Law Enforcement Liaison & Disclosures) who had previously given oral evidence to the Committee, Jerry Butcher (Law Enforcement Liaison Manager, Bristol), Paul Fennelly (Law Enforcement Liaison Manager, Hatfield), David Frank (Public Affairs Manager) and Vanessa Mortiaux (Senior Legal Counsel)

3. Mr Grayling made a presentation to the Committee. He explained that EE prefers requests for communications data to be made under RIPA rather than other legislation which is available to some public bodies. He referred to the use by local authorities of the National Anti-Fraud Network and to the good relations which EE had with SPoCs and with the security services who submitted high quality requests. He explained that where requests were submitted to EE under RIPA, the onus was on the requesting body to check that its request was necessary and proportionate—it was not for EE to make that judgment.

4. Mr Grayling explained that his team had responsibilities to customers to safeguard data, to minimise costs and ensure a level playing field, and an overarching corporate social responsibility. They worked closely with the Government, including meeting regularly with the Home Office, and valued their partnership. But they were concerned that the draft Bill was so wide-reaching, and did not state on its face what would be required of them. He looked forward to further consultation with the Home Office.

5. The costs recovery provisions under RIPA worked well, and had not so far caused problems.

6. The Committee visited the office where requests for communications data were received, and discussed the procedure with Sheena Wright, the Police Liaison Team Leader, and other EE representatives. They indicated that from their perspective the SPoC system worked well. It involved dedicated teams and relationships based on trust.

Appendix 6: Memorandum from Delegated Powers Committee

The Joint Committee sought the Delegated Powers Committee's views on the draft Bill, in particular on clauses 1, 9 and 21. Our conclusions are as follows.

General approach

8. The Committee viewed clauses 1, 9 and 21 not just as separate items, but also as an integrated whole. The cumulative effect of the delegated powers in the draft Bill add to their individual significance, and we understand why they may be of concern to the Joint Committee. For example, the significance of clause 1 would be less if Part 2 of the Bill was more restrictive of the ability of public authorities to access the data which was required to be held and ensured effective remedies and protection for the citizen. We were concerned that the draft Bill lacked sufficient clarity in defining the scope and potential use of delegated powers; and that the delegated powers memorandum lacked sufficient justification for the powers contained in the draft Bill.

9. The fact that aspects of the power may be insufficiently clearly defined will of course impact on other aspects of the draft Bill which the Joint Committee may consider, such as the efficacy of the remedies provided in the Bill for breaches of its requirements, not just for telecommunications operators, but also for those whose data is held. We recognise the importance of the problems this legislation seeks to address but precisely because of its gravity we are concerned that the legislation should be tightly drawn to avoid the need for delegated powers being inappropriately used.

Clause 1 – Availability of communications data

10. Clause 1(1) enables the Secretary of State, by order subject to affirmative procedure, to ensure that communications data (defined in clause 28 on page 59 of the Command Paper) is available to be obtained from telecommunications operators by relevant public authorities in accordance with Part 2, or otherwise to facilitate the availability of communications data to be so obtained. Clause 1(2) and (3) give examples of things for which the order may in particular provide, though they do not limit the extent of the power. But the examples are significant – for instance, it is clear that an order may require an operator to collect information for which it would have no use in the ordinary course of its business.

11. One of the things which an order can do is provide for the imposition of requirements or restrictions on telecommunications operators by notice of the Secretary of State. When that happens, the draft Bill provides a mechanism for referral to the Technical Advisory Board (clause 7) and for enforcement (by civil proceedings - clause 8). The draft Bill is silent as to any enforcement of requirements imposed by the order itself, rather than by notice under the order.

12. There are provisions in the draft Bill dealing with the security of data (clause 3), the period for its retention (clause 4), access to it (clause 5) and its destruction (clause 6). But

the draft Bill contains no coherent framework for what, or whose, data is to be collected or generated or to what requirements the telecommunications operators will be subject. Paragraph 6 of the memorandum gives as the reason for this the need for flexibility, but this does not necessarily justify the potentially very intrusive nature of the requirements that may be imposed by an order under clause 1. There are possibly very significant implications not just for the telecommunications operators but also for every person whose communications data may be required to be obtained and held (and so would be accessible under Part 2 for any of a number of purposes, not just combating crime, let alone serious crime). We do not consider that it is appropriate to delegate to the Secretary of State the power, subject to so limited a framework, to establish a regime which could amount to wholesale general retention of subscriber, traffic and use data about the population at large. We consider that the regulatory structure for the scheme should be in the Bill itself, even though the details of particular requirements for particular operators might be left to subordinate legislation or a notice procedure for which the Bill itself would provide.

Clause 9(7) – Permitted purposes

13. This Henry VIII power to make orders essentially reproduces section 22(2)(h) of the Regulation of Investigatory Powers Act 2000 ("RIPA"). It enables the Secretary of State to add to or restrict the permitted purposes for which communications data may be obtained. The orders are subject to affirmative procedure.

14. In relation to the Bill which became RIPA, our Committee recommended that the equivalent power should be restricted to the two purposes for which the then government said it may wish to use it. But the House did not amend the Bill despite that recommendation. There is a limitation on the power in that it cannot be exercised incompatibly with the Convention rights under the Human Rights Act 1998 (as explained in paragraphs 8 and 9 of the Department's memorandum), and the use which has been made of the equivalent power under RIPA is limited. But the significance of this power is all the greater because of the effect of Part 1 and, were a Bill to be introduced containing the same power as in the draft, we would not necessarily find it acceptable just because it derives from existing legislation.

Clause 21(1), (7) and (8) – Relevant public authorities

15. These powers enable the Secretary of State to alter the list of relevant public authorities, that is those authorities whose senior officers may authorise obtaining data under Part 2 of the draft Bill. An order is subject to affirmative procedure if it designates a new authority or consequentially amends primary legislation. Otherwise, the orders are subject to negative procedure. Both the powers and the procedure follow section 25(1), (4) and (5) of RIPA.

16. In relation to the Bill which became RIPA, our Committee recommended that the order making powers should be restricted to making changes that are necessary as a consequence of changing structures within an authority. The House did not amend the Bill despite that recommendation and the power in RIPA has been used to add well over 20 authorities to the list. The draft Bill would repeal the relevant provisions in RIPA and the Joint Committee may perhaps wish to question the uses to which the equivalent new powers will be put, bearing in mind that paragraph 38 of the memorandum says that the

powers will most commonly be used to address changes consequent on the abolition of a body or the transfer of its functions to a successor. The use to which the existing powers have been put does not seem to have been so limited. We share the doubts of our predecessor committee about the appropriateness of so open-ended a delegation.

18 October 2012

Appendix 7: Procedure for super-affirmative resolution

Future proofing and Parliamentary oversight

1. If clause 1 is to be narrowed then it is necessary to consider what should happen if changes are needed in the future.

2. The Home Office wishes to future proof the Bill and this will inevitably require either very broad powers which the Secretary of State can exercise herself (as in the current clause 1), or a narrower set of powers in clause 1 combined with a significant delegation of legislative power to the Secretary of State to enable her (and her successors) to make an order to widen clause 1 if and when necessary. The other option is not to future proof the Bill and simply to accept future primary legislation may be necessary.

The super-affirmative procedure

3. The super-affirmative procedure is set out under section 18 of the Legislative and Regulatory Reform Act 2006. Briefly it is as follows. The Minister has a statutory duty to consult (section 13) and must lay before Parliament an explanatory memorandum for the order including, among other things, details of the consultation (section 14). The Minister cannot make the order for 60 days from the date it is laid not including periods when either House is adjourned for more than 4 days. Within the 60 days a Committee of either House charged with reporting on the draft order can recommend that no further proceedings be taken on the order, can make recommendations for amendment of the draft order or could clear it without making recommendations. The minister must have regard to any resolutions or recommendations, or any other representations made during the 60 days. After the 60 days has elapsed, the Minister can either proceed with the draft order without amendment or lay a revised draft order, and then there is a further process of non-time limited committee scrutiny and affirmative approval by both Houses. A Committee of either House can thus block an order if it believes that, even if amended, it is still unsatisfactory. Only a resolution of the relevant House can overturn the Committee's recommendation.

4. This procedure pre-supposes that at least one House either already has a Committee designated and able to scrutinise the draft order or that it is prepared to set up such a Committee any time an order is laid. It might be appropriate to recommend the formation of a Joint Committee (although this would ultimately be a matter for the two Houses). However, a government with a majority could block the setting up of such a Committee. If a special committee has to be appointed once an order was laid this would take a chunk of time out of the 60 day scrutiny period: it always takes at least two or three weeks to set up a joint committee and often it takes significantly longer.

Is the super-affirmative procedure quicker than requiring new primary legislation?

5. The super-affirmative procedure is not necessarily quicker than the primary legislative route. The Home Office says primary legislation is too slow and they need a quicker way to widen clause 1. But emergency or fast-track primary legislation can be passed in a few days, and even non-emergency legislation can be passed within a few months (if it can get a place in the legislative programme or can be added to other another Bill).

6. The super-affirmative procedure could go on for a long time under the super-affirmative process. For example, if an order had been laid on 16 July 2012 the 60 day scrutiny period (taking into account recess dates in both Houses) would run until January 2013, then there would need to be time for HMG to consider recommendations/representations, come forward with the original or a revised order, further committee scrutiny and motions in both Houses. All in all it could potentially take 8-9 months.

Appendix 8: Abbreviations and acronyms

ACPO	Association of Chief Police Officers
CD	Communications Data
CEOP	Child Exploitation and Online Protection Centre
CIU	(Metropolitan Police) Communications Intelligence Unit
CPS	Crown Prosecution Service
CSP	Communication Service Provider
DPA	Data Protection Act 1998
DPI	Deep Packet Inspection
DRD	EU Data Retention Directive
DSO	Designated senior officer
ECHR	European Convention on Human Rights
EE	Everything Everywhere
FSA	Financial Services Authority
GCHQ	Government Communications Headquarters
GPRS	General packet radio service
HMRC	Her Majesty's Revenue and Customs
IC	Information Commissioner
ICO	Information Commissioner's Office
IoCC	Interception of Communications Commissioner
IP	Internet protocol
ISC	Intelligence and Security Committee
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
LEA	Law Enforcement Authorities
LGA	Local Government Association
LINX	London Internet Exchange
MLAT	Mutual Legal Assistance Treaty

MPS	Metropolitan Police Service
NAFN	National Anti-Fraud Network
RIPA	Regulation of Investigatory Powers Act 2000
SCDEA	Scottish Crime and Drug Enforcement Agency
SFO	Serious Fraud Office
SOCA	Serious Organised Crime Agency
SMS	Short message service
SPoC	Single Point of Contact
UKBA	UK Border Agency

Appendix 9: Formal Minutes

Wednesday 28 November 2012

Present:

Lord Blencathra, in the Chair

Lord Armstrong of Ilminster	Mr Nicholas Brown MP
Baroness Cohen of Pimlico	Mr Michael Ellis MP
Lord Faulks	Dr Julian Huppert MP
Lord Jones	Mr Stephen Mosley MP
Lord Strasburger	Mr Craig Whittaker MP
	Mr David Wright MP

Draft Report (*Draft Communications Data Bill*), proposed by the Chair, brought up and read.

Ordered that the draft Report be read a second time.

Paragraphs 1 to 326 read and agreed to.

Summary agreed to.

Appendices to the Report agreed to.

Resolved, That the Report be the Report of the Committee to both Houses.

Written evidence was ordered to be reported.

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No. 134 of the House of Commons.

The Committee adjourned.